

COMPUTAZIONE QUANTISTICA

ATOMO DI IDROGENO ($\frac{1}{2} \cdot 10^{-10} \text{ m} = \frac{1}{2} \text{ Å}$)

APPLICAZIONI

- Branconote quantistiche → non sono fabbricabili
- Teletrasporto
- Crittografia Quantistica
- Circuiti quantistici
- TF quantistica (Transformata di Fourier)
- Grover (Ricerca in un DB non strutturato)

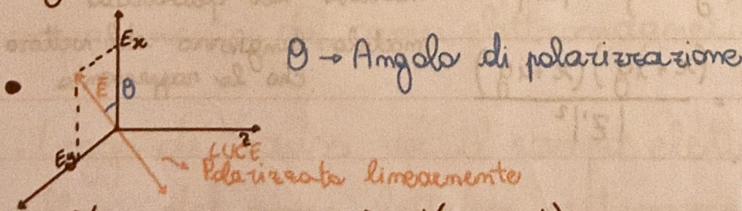
BIT QUANTISTICI quantum bits QUBITS

QUBITS → Gli stati si sovrappongono

- Multiple qubits
- Porte quantistiche → cambiano lo stato solo bit

LEGGE DI GORDON MOORE

ogni 18 mesi si dimezzano le dimensioni dei chip



$$\vec{E}(x, y, z, t) = \vec{E}_0 e^{i(kz - \omega t)}$$

→ vettore che dipende da posizione e tempo

→ CAMPO ELETTRICO

ESISTE UN'ALGORITMO CHE RENDE CUBICO IL CALCOLO DEI NUMERI PRIMI (gli algoritmi RSA saranno inutili)

$$k = \frac{2\pi}{\lambda}$$

NUMERI COMPLESSI

$$ax + b = 0$$

$$a, b \in \mathbb{Z} \quad x = -\frac{b}{a} \rightarrow x \in \mathbb{Q}$$

$\sqrt{2} \in \mathbb{R} \rightarrow$ non è rappresentabile come $\frac{a}{b}$ (caso di irrazionalità)

$$x^2 = -1 \rightarrow \sqrt{-1} \rightarrow x \in \mathbb{C} \quad \sqrt{-1} = i \text{ (Unità Immaginaria)}$$

$$\frac{ax^2 + bx + c = 0}{x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}}$$

se $\Delta < 0$

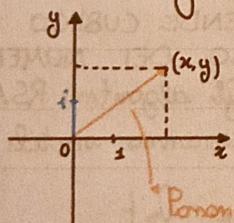
$$\Delta = b^2 - 4ac \quad -\Delta = -b + 4ac > 0$$

$$x = \frac{-b \pm \sqrt{-\Delta}}{2a} = \frac{-b \pm \sqrt{-1} \cdot \sqrt{\Delta}}{2a} = \frac{-b \pm i \cdot \sqrt{\Delta}}{2a}$$

$$z = x + iy \quad x, y \in \mathbb{R}$$

OPERAZIONI

$$z = x + iy \quad z' = x' + iy' \quad \text{se solo } y \text{ allora immaginari puri}$$



- SOMMA $z + z' = x + x' + i(y + y')$

Potendo essere rappresentati
come vettori

- PRODOTTO $z \cdot z' = (x + iy)(x' + iy') = xx' + ix y' + iy x' + i^2 y y' = xx' - yy' + i(xy' + x'y)$

$$z'^* = x' - iy' \text{ (coniugato)} \quad z' \cdot z'^* = x'^2 + y'^2 = \rho^2 = |z'|^2 \rightarrow \text{modulo al quadrato}$$

- DIVISIONE $\frac{z}{z'} = \frac{(x+iy)}{(x'+iy')} \cdot \frac{(x'-iy')}{(x'-iy')} = \frac{(x+iy)(x'-iy')}{|z'|^2}$

modulo = lunghezza del vettore
che lo rappresenta

$$\lim_{h \rightarrow 0} \frac{f(x+h) - f(x)}{h} = \frac{df(x)}{dx}$$

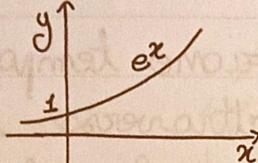
Sviluppo di Taylor

$$f(y+x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!} (x-a)^n$$

$y \rightarrow$ numero reale o complesso

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

$$\frac{de^x}{dx} = e^x$$



$e =$ costante di EULERO

$$e^x = e^{(0+x)} = 1 + x + \frac{x^2}{3!} + \dots + \frac{x^n}{n!}$$

se al posto di x prendo un'immaginario puro (i)

$$e^{ix} = 1 + ix + \frac{(ix)^2}{2!} + \frac{(ix)^3}{3!} + \frac{(ix)^4}{4!} + \dots + \frac{(ix)^n}{n!}$$

$$1 + ix - \frac{x^2}{2!} - \frac{ix^3}{3!} + \frac{x^4}{4!} +$$

- Parte immaginaria

- Parte reale

$$e^{ix} = \cos x + i \sin x$$



FORMULA DI EULERO

$$e^{i\pi} = -1 = e^{i\pi} + 1 = 0$$

EQ. MAXWELL

Sono un insieme di 4 equazioni che descrivono il comportamento dei campi elettromagnetici.

1. Legge di Gauss per il campo elettrico: la somma dei flussi del campo elettrico attraverso una superficie chiusa è proporzionale alla carica contenuta all'interno di quella superficie divisa per la costante dielettrica del vuoto

OPERATORE
NABLA

$$\leftarrow \nabla E = \rho / \epsilon_0$$

→ CAMPO ELETTRICO
↓ DENSITÀ DI CARICA

2. Legge di Gauss per il campo magnetico: il flusso del campo magnetico attraverso una superficie chiusa è sempre nullo.

$$\nabla \cdot \vec{B} = 0$$

→ CAMPO MAGNETICO

3. Legge di Faraday: la variazione temporale del flusso del campo magnetico, attraverso una superficie aperta, genera un campo elettrico circolare lungo il bordo di quella superficie.

$$\nabla \times \vec{E} = -\frac{d\vec{B}}{dt}$$

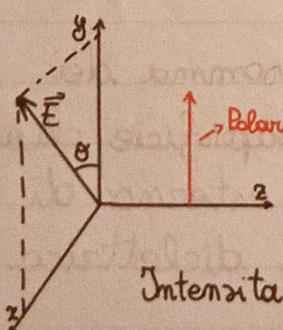
4. Legge di Ampère-Maxwell: la somma di un termine di corrente elettrica genera una circolazione del campo magnetico lungo il bordo di una superficie aperta

$$\nabla \times \vec{B} = \mu_0 (j + \epsilon_0 (\frac{d\vec{E}}{dt}))$$

→ PERMEABILITÀ MAGNETICA
↓
COSTANTE DIELETTRICA DEL VUOTO

FOTONI

campo elettrico $\vec{E} = E_x \sin\theta \hat{x} + E_y \cos\theta \hat{y} = E \sin\theta \cos(\omega t) \hat{x} + E \cos\theta \sin(\omega t) \hat{y}$



$$= \sin\theta \Psi_x + \cos\theta \Psi_y$$

Polarizzazione orizzontale

Polarizzazione verticale

Intensità $\propto E^2$

$$\omega = \frac{2\pi}{T} \quad c = \frac{\omega\lambda}{2\pi} \quad \omega = 2\pi\nu$$

POLARIZZATORE \rightarrow uccide le componenti orizzontali

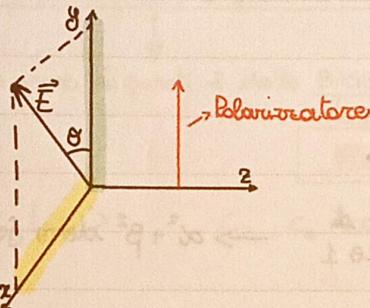
E^2 dopo il polarizzatore $= E^2 \cos^2 \theta$ \hookrightarrow dipende da θ \rightarrow LEGGE DI MALUS

Intensità dopo il polarizzatore $E^2 \cos^2 \theta$

$$\vec{E} = \sin \theta E \cos \omega t \hat{x} + \cos \theta E \cos \omega t \hat{y}$$

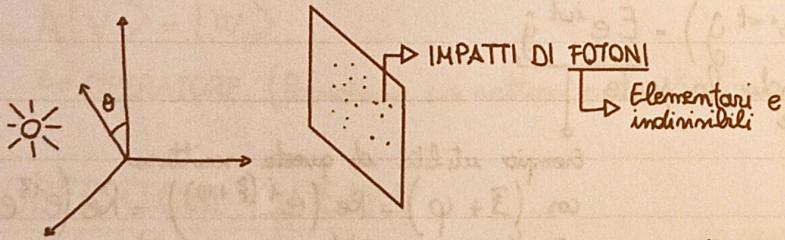
$$\vec{E} = \sin \theta \Psi_x + \cos \theta \Psi_y$$

radiante
per orizzontale
 $\theta = 90^\circ$ radiante
per verticale
 $\theta = 0^\circ$



come si riduce l'intensità dopo un polarizzatore

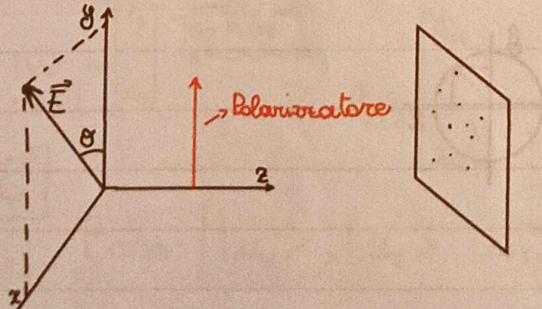
si riduce di un fattore $\cos^2 \theta$



collegamento tra INTENSITÀ e n° di impatti

$\Rightarrow E(x, y, z, t) =$ PROBABILITÀ DI TROVARE UN FOTONE IN x, y, z, t
 \hookrightarrow La probabilità è proporzionale all'intensità

SE AGGIUNGO UN POLARIZZATORE



non passeranno tutti i FOTONI
ma solo uno % ($\cos^2 \theta$)

FOTONE POLARIZZATO ORIZZONTALMENTE = 0 }
FOTONE POLARIZZATO VERTICALMENTE = 1 } nono VETTORI

VETTORI → In meccanica quantistica il vettore si rappresenta così: $|0\rangle, |1\rangle$

↳ VETTORE CHE DESCRIVE UN FOTOONE POLARIZZATO ORIZZONTALMENTE

$$|0\rangle = \cos\theta |0\rangle + \sin\theta |1\rangle$$

PRINCIPIO DI SOVRAPPOSIZIONE QUANTISTICA

DEFINIZIONE DI QUANTUMBIT

QUBIT

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

α^2 prob di ottenere 0 β^2 prob di ottenere 1 $\rightarrow \alpha^2 + \beta^2$ deve fare 1

$$1. e^{i\varphi} = \cos\varphi + i\sin\varphi$$

Gli esponenti possono essere complessi se abbiamo un campo elettrico che oscilla

$$\vec{E} = E \cos\omega t \hat{y} = \operatorname{Re}(E e^{i\omega t} \hat{y}) = E e^{i\omega t} \hat{y}$$

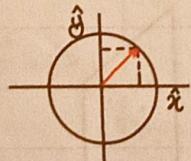
↳ Prendiamo la parte reale

Esempio utilità di questa scrittura
 $\cos(\beta + \varphi) = \operatorname{Re}(e^{i(\beta + \varphi)}) = \operatorname{Re}(e^{i\beta} e^{i\varphi})$
 $= \operatorname{Re}((\cos\beta + i\sin\beta)(\cos\varphi + i\sin\varphi)) =$
 $= \operatorname{Re}(\cos\beta\cos\varphi + i(\cos\beta\sin\varphi + \sin\beta\cos\varphi) - \sin\beta\sin\varphi)$
 $= \cos\beta\cos\varphi - \sin\beta\sin\varphi$

Fotone sfarzato

$$|\rightarrow\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$$

$$\frac{E}{\sqrt{2}} \cos\omega t \hat{y} + \underbrace{\frac{E}{\sqrt{2}} \cos\left(\omega t + \frac{\pi}{2}\right)}_{\sin\omega t} \hat{x}$$



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

$$\alpha^*\alpha$$

$$|\alpha|^2$$

ALGEBRA LINEARE

- $|v\rangle$: vettore in spazi vettoriale COMPLESSI
- VETTORI LINEARMENTE INDIPENDENTI (se ho n vettori sono linearmente indipendenti se non possono essere espressi come combinazione lineare degli altri)
- MASSIMO NUMERO DI VETTORI LINEARMENTE INDIPENDENTI = DIM SPAZIO

Un insieme di questi è detto BASE

→ POSSO DESCRIVERE TUTTI GLI ALTRI CON QUELLI DELLA BASE

$$\cdot |v\rangle = c_1|u_1\rangle + c_2|u_2\rangle + \dots + c_n|u_n\rangle \quad c_1 \dots c_n = \text{COMPONENTI DI } |V\rangle$$

$$|v\rangle = \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}$$

$$\cdot A|v\rangle = |w\rangle$$

↳ OPERATORE (Premettono un vettore e lo trasformano in un altro)

OPERATORI LINEARI

$$1. A(c_1|u_1\rangle + c_2|u_2\rangle + \dots + c_n|u_n\rangle) = c_1A|u_1\rangle + \dots + c_nA|u_n\rangle = A \sum_{i=1}^n c_i|u_i\rangle$$

↳ È rappresentabile con una matrice

2. RAPPRESENTAZIONE MATRICIALE di vettori e operatori

$$|v\rangle \rightarrow \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} \quad \begin{array}{l} \text{matrice non} \\ n \rightarrow \text{RIGHE} \\ 1 \rightarrow \text{COLONNA} \end{array}$$

$$A \rightarrow \begin{bmatrix} A_{11} & \dots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{n1} & \dots & A_{nn} \end{bmatrix} \quad A|u_i\rangle = \begin{bmatrix} A_{1i} \\ \vdots \\ A_{ni} \end{bmatrix}$$

$$\sum_{i=1}^n a_{ri} A|u_i\rangle$$

C^3

Base: $\{|u_1\rangle, |u_2\rangle, |u_3\rangle\}$

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

$$A|u_2\rangle = 4|u_1\rangle + 2|u_3\rangle$$

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

$$A = \begin{bmatrix} 0 & 4 & 3 \\ 2 & 2 & 0 \\ -i & 0 & 4 \end{bmatrix}$$

ES.

$$A(6|\mu_1\rangle + 5|\mu_2\rangle + |\mu_3\rangle) \rightarrow \begin{bmatrix} 0 & 4 & 3 \\ 2 & 2 & 0 \\ -1 & 0 & 4 \end{bmatrix} \begin{bmatrix} 6 \\ 5 \\ 1 \end{bmatrix} = \begin{bmatrix} 23 \\ 22 \\ 4-6i \end{bmatrix}$$

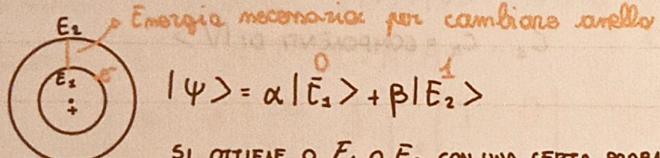
SOMMA E PRODOTTO DI OPERATORI

$$(A+B)|v\rangle \equiv A|v\rangle + B|v\rangle \rightarrow \text{MATERICI } (A+B) = M(A) + M(B)$$

$$(AB)|v\rangle \equiv A(B|v\rangle) \rightarrow \begin{array}{l} \text{si fanno in sequenza} \\ (\text{primo quello a destra}) \end{array} \rightarrow AB \neq BA \rightarrow \text{NON è commutativo}$$

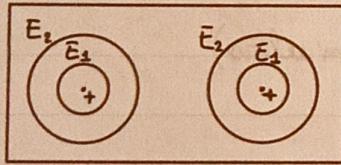
MATRICI DI PAULI (se ne moltiplica 2) $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

ESEMPI DI QUBIT



SI OTTIENE O E_1 O E_2 CON UNA CERTA PROBABILITÀ

$$P(E_1) = |\alpha|^2 \quad P(E_2) = |\beta|^2$$



MISURA E	
1° Atomo	2° Atomo
E_1	E_1
E_1	E_2
E_2	E_1
E_2	E_2

$$\begin{aligned} |E_1\rangle|\bar{E}_1\rangle \\ |E_1\rangle|E_2\rangle \\ |E_2\rangle|\bar{E}_1\rangle \\ |E_2\rangle|E_2\rangle \end{aligned}$$

CASO IN CUI
ENTRAMBI SONO
IN UNO STATO
DEFINITO

$$|\Psi\rangle = \alpha|E_1\rangle + \beta|E_2\rangle$$

$$|\chi\rangle = \gamma|\bar{E}_1\rangle + \delta|E_2\rangle$$

$$P(E_1, E_2) = |\alpha|^2 |\gamma|^2 \dots \text{ecc... per le altre } P$$

$$|\Psi\rangle = \alpha\gamma|E_1\rangle|E_1\rangle + \alpha\delta|E_1\rangle|E_2\rangle + \beta\gamma|E_2\rangle|E_1\rangle + \beta\delta|E_2\rangle|E_2\rangle \rightarrow \text{COMBINAZIONE DI 2 QUBIT}$$

$2^n \rightarrow$ stati possibili $n \rightarrow n^{\circ}$ QUBIT

La misurazione di un QUBIT disturba il suo stato quantistico, che collassa in uno dei suoi stati di base dopo la misura. Il collasso della funzione d'onda causerà la perdita della sovrapposizione quantistica. ($|\alpha|^2$ probabilità $|0\rangle$ e $|\beta|^2$ probabilità $|1\rangle$)

LEZIONE 3

Funzione d'onda

$$|\Psi\rangle = \Psi(x)|x\rangle + \Psi(x')|x'\rangle + \Psi(x'')|x''\rangle \dots = \int \Psi(x)|x\rangle dx$$

RIPASSO ALGEBRA LINEARE

Tutti i vettori sono esprimibili
tramite i vettori

$$\begin{array}{c} \text{103} \\ \downarrow \\ \text{103} \end{array} \quad |v\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$$

OGNI VETTORE DIPENDERÀ DALLA BASE

- Oggetti che trasformano i vettori in un numero (molti non ricordati)

OPERATORI (continuazione)

$$\bullet AB - BA = [A, B] \text{ COMMUTATORE}$$

esercizio $[T_1, T_2]$

$$\bullet \text{OPERATORE } I \text{ (Identità)} \quad I|v\rangle = |v\rangle \quad \# |v\rangle = \begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix}$$

$$\bullet \text{INVERSO } A^{-1} \quad A \cdot A^{-1} \cdot I = A^{-1}A$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x & y \\ z & w \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{cases} ax + bz = 1 \\ ay + bw = 0 \\ cx + dz = 0 \\ cy + dw = 1 \end{cases}$$

Perché se il
determinante è ≠
da 0 M è invertibile

$$\frac{1}{ad-bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \frac{\begin{bmatrix} ad-bc & 0 \\ 0 & -cb+ad \end{bmatrix}}{ad-bc}$$

$$[A, I] = 0$$

$$0 \cdot A = 0 \quad A + 0 = A$$

$\langle v | v \rangle \rightarrow$ prodotto scalare
di un vettore × se stesso
rappresenta la norma
al quadrato $\|v\|^2$
 $\langle v | v \rangle = v_1 v_1 + v_2 v_2 + \dots + v_n v_n$
 se $[A, B] = 0$ allora $AB = BA$

PRODOTTO SCALARE

$$\vec{v} \cdot \vec{w} = |\vec{v}| \cdot |\vec{w}| \cdot \cos \theta \quad \overrightarrow{v} \overrightarrow{w}$$

Il prodotto scalare tra due vettori è un numero reale

$$\vec{v} \cdot \vec{w} = v_1 w_1 + v_2 w_2 + v_3 w_3$$

Prodotto scalare in spazi vettoriali complessi
 $(|v\rangle, |w\rangle) \in \mathbb{C}$

i) Se scambio primo con secondo vettore otengo complesso coniugato

$$(|v\rangle, |w\rangle) = (|w\rangle, |v\rangle)^*$$

$$ii) \quad (|\Psi\rangle, c_1|v\rangle + c_2|w\rangle) = c_1(|\Psi\rangle, |v\rangle) + c_2(|\Psi\rangle, |w\rangle)$$

$$(c_1|v\rangle + c_2|w\rangle, |\psi\rangle)^*$$

$$iii) (C_1|V\rangle + C_2|W\rangle, |\Psi\rangle) = C_1^*(|\Psi\rangle, |V\rangle) + C_2^*(|\Psi\rangle, |W\rangle)$$

iv) $(|\Psi\rangle, |\Psi\rangle) = (\Psi, \Psi)^*$ → quindi numero reale $Z = Z^* \in \mathbb{R}$
 $\geq 0 \rightarrow = 0$ se $|\Psi\rangle$ è il vettore nullo

- Lunghezza o norma di un vettore \rightarrow PITAGORA
 $(|v\rangle, |v\rangle) = \|v\|^2$
La Norma

ORTOGONALITÀ TRA VETTORI

$|v\rangle$ e $|w\rangle$ sono ortogonali s.s.e. $(|v\rangle, |w\rangle) = 0$

- Poco trovare una base con vettori ortogonali tra loro

$$(|u_i\rangle, |u_j\rangle) = 0 \text{ as } i \neq j$$

- Sarebbe anche bello che avessero lunghezza $t \rightarrow \frac{IV}{VII}$

In questo caso ho una BASE ORTOGONALE

- $$\text{- Base orthonormale } \{|\mu_i\rangle\} \quad (|\mu_i\rangle, |\mu_j\rangle) = \delta_{ij} \quad \text{Kronecker}$$

$$\langle \mu_i | \mu_s \rangle$$

KET viene usato per rappresentare il
rettore colonna.
BRA transposto coniugato di ket

Componente di un vettore lungo $|M_i\rangle \rightarrow (|M_i\rangle, |v\rangle) = V_i$

$$A_{ij} = \langle \mu_i | A | \mu_j \rangle$$

$$-(|v\rangle, |w\rangle) = \langle v^* | M_3 \rangle, v^* | u_2 \rangle \dots, w_3 | u_3 \rangle \dots w_n | u_1 \rangle$$

$$V_1^* W_1 + V_2^* W_2 \dots + V_n^* W_n$$

TRASPOSIZIONE (Scambio di righe con colonne)

$$A_{ij} \rightarrow A_{ji}$$

OPERATORE AGGIUNTO (Trasporto coniugato)

$$(\Psi), A|\Phi\rangle = (A^*|\Psi\rangle, |\Phi\rangle) \rightarrow \text{Def}$$

$$(A^*)_{ij} = (\mu_i), A^*|\mu_j\rangle *$$

$$(\Psi), A^*|\Phi\rangle = (A|\Psi\rangle, |\Phi\rangle)$$

$$* = \left[A|\mu_i\rangle, |\mu_j\rangle \right] = \\ = \left[|\mu_j\rangle, A|\mu_i\rangle \right]^* = A_{ji}^*$$

Prodotto interno tra $A v$ e u è uguale al prodotto interno tra v e il trasporto coniugato di A (A^*)

$$\langle u, Av \rangle = \langle A^* u, v \rangle$$

Nelle matrici R corrispondono alle rotazioni

PORTE LOGICHE QUANTISTICHE

Le porte logiche sono operatori unitari

$$U^\dagger U = I = U U^\dagger$$

↪ mantengono i prodotti scalari

$$(|v\rangle, |w\rangle) \rightarrow (U|v\rangle, U|w\rangle) = (|v\rangle, U^\dagger U|w\rangle) = (|v\rangle, |w\rangle)$$

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

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

$$\Leftrightarrow (|\Psi\rangle, |\Psi\rangle) = 1$$

U = operatore unitario
 $\langle Ux|Uy \rangle = \langle xy \rangle$

↪ Dobbiamo impostare che i vettori che descrivono QUBIT abbiano norma uguale a 1 e si deve mantenere uguale a 1

MQ

I: lo stato \rightarrow vett. ket $|\Psi\rangle$

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

Autostati o autovettori $P(\alpha) = |\alpha|^2$ $P(\beta) = |\beta|^2$

$$\langle \Psi, \Psi \rangle = 1$$

III: $|\Psi\rangle \xrightarrow{\text{misura}} |z\rangle \rightarrow$ Dopo la misura un QUBIT diventa un bit classico

PORTE QUANTISTICHE (A singolo QUBIT)

4 Porte CLASSICHE

$a \xrightarrow{\quad} a$

$a \xrightarrow{\square} \bar{a}$ NOT

$a \xrightarrow{\square} 0$

$a \xrightarrow{\square} 1$

$|0\rangle |1\rangle$

$\boxed{?}$

LE PORTE LOGICHE QUANTISTICHE SONO MATERICI

NOT

$$|0\rangle \rightarrow \boxed{\quad} \rightarrow |1\rangle$$

$$|1\rangle \rightarrow \boxed{\quad} \rightarrow |0\rangle$$

$$\text{NOT } |0\rangle = |1\rangle \rightarrow \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \rightarrow X = \text{NOT} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$X(\alpha|0\rangle + \beta|1\rangle) = \alpha X|0\rangle + \beta X|1\rangle = \alpha|1\rangle + \beta|0\rangle$$

CI SONO INFINITE MATRICI UNITARIE PER UN QUBIT

NOTA: $U_1 \cdot U_2 \rightarrow$ il prodotto di un operatore unitario è un operatore unitario? SI

$$(U_1 U_2)^* = U_1^* U_2^*$$

$$(U_1 U_2)^{-1} = U_2^{-1} U_1^{-1}$$

$$U_1 \boxed{U_2 U_2^{-1}} U_1^{-1} = I$$

\downarrow
COMPOSIZIONE DI PORTE
LOGICHE È UNA PORTA
LOGICA

*1

$$(AB)^T = B^T A^T \rightarrow \sum_k B_{ik}^T A_{kj}^T$$

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

$$(AB)_{ij}^T = (AB)_{ji} = \sum_k A_{jk} B_{ki}$$

$$U = e^{i\alpha} \begin{pmatrix} e^{-\frac{i\beta}{2}} & 0 \\ 0 & e^{\frac{i\beta}{2}} \end{pmatrix} \begin{pmatrix} \cos \frac{\gamma}{2} & -\sin \frac{\gamma}{2} \\ \sin \frac{\gamma}{2} & \cos \frac{\gamma}{2} \end{pmatrix} \begin{pmatrix} e^{-\frac{i\delta}{2}} & 0 \\ 0 & e^{\frac{i\delta}{2}} \end{pmatrix}$$

\rightarrow Infinità di
porte quantistiche
unitarie

NOTA:

NELLA COMPUTAZIONE QUANTISTICA NON POSSO Duplicare UN QUBIT

$$X = \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} \quad Y = \begin{vmatrix} 0 & -i \\ i & 0 \end{vmatrix} \quad Z = \begin{vmatrix} 1 & 0 \\ 0 & -1 \end{vmatrix} \quad H = \frac{1}{\sqrt{2}} \begin{vmatrix} 1 & 1 \\ 1 & -1 \end{vmatrix} \quad \rightarrow \text{PORTE A UN QUBIT PRINCIPALI}$$

PORTE A DUE QUBITS

$$4 \text{ Stati di Base } |\Psi\rangle = \alpha|0\rangle|0\rangle + \beta|0\rangle|1\rangle + \gamma|1\rangle|0\rangle + \delta|1\rangle|1\rangle \quad |\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$$

BASE COMPUTAZIONALE (con 2 QUBIT)

Def Non sempre lo stato generale di un QUBIT è scrivibile come prodotto
 $(\alpha|0\rangle + \beta|1\rangle) (\gamma|0\rangle + \delta|1\rangle)$

$$\alpha\gamma|0\rangle|0\rangle + \alpha\delta|0\rangle|1\rangle + \beta\gamma|1\rangle|0\rangle + \beta\delta|1\rangle|1\rangle$$

\downarrow
Potrebbe essere o non
non scrivibile

es. $|0\rangle|0\rangle + |1\rangle|1\rangle$
 (non trovi $(\alpha, \beta, \gamma, \delta)$ per rappresentarlo)

STATO ENTANGLED

Algebra

- Vettori: $|v\rangle$ "Ket" \rightarrow Vettori che indicano stati nella meccanica quantistica

$$\alpha|v\rangle + b|w\rangle + \dots + d|z\rangle = 0$$

$\Rightarrow \alpha = b = \dots = d = 0 \rightarrow$ linearmente indipendenti.

se non tutti nulli allora \rightarrow linearmente dipendenti

- base $\{|u_i\rangle\}$ $n = \dim$ spazio (massimo numero di vettori linearmente indipendenti)

$$|v\rangle = \sum_i v_i |u_i\rangle$$

\hookrightarrow Se non linearmente indipendenti si ponono
soluzioni come combinazioni lineari

es.

$$\alpha \begin{bmatrix} 1 \\ 1 \end{bmatrix} + b \begin{bmatrix} -3 \\ 2 \end{bmatrix} = 0 \rightarrow \begin{cases} \alpha - 3b = 0 \\ \alpha + 2b = 0 \end{cases} \rightarrow \alpha = b = 0 \rightarrow \text{LINEARMENTE INDIPENDENTI}$$

$$5. \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 2 \\ -1 \end{bmatrix}, \begin{bmatrix} 0 \\ -1 \\ 1 \end{bmatrix} \quad \text{NO LINEARMENTE INDIPENDENTI}$$

$$|v\rangle - |w\rangle = |z\rangle$$

- Prodotto scalare $\langle v|w\rangle \in \mathbb{C}$

$$\langle v|v\rangle \in \mathbb{R} \text{ e } \geq 0$$

$$\|v\| = \sqrt{\langle v|v\rangle} \text{ NORMA}$$

vettori orthonormali

$$\langle |v\rangle, |w\rangle = \sum_i \sum_j v_i^* w_j \langle |u_i\rangle |u_j\rangle$$

$$\delta_{ij} \rightarrow 0 \text{ se } i=j \text{ e } \infty \text{ se } i \neq j$$

$$\langle |v\rangle, |v\rangle = \sum_i v_i^* v_i = \sum_i |v_i|^2$$

- OPERATORI $A|v\rangle = |w\rangle$

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

L'OPERATORE LINEARE

MQ

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow \text{REGOLA DI BORN}$$

$$\langle |\psi\rangle, |\psi\rangle = \alpha^* \alpha + \beta^* \beta = |\alpha|^2 + |\beta|^2 = 1$$

vettore che rappresenta uno stato finito

$$\langle \psi | \psi \rangle = 1 \rightarrow$$

- OP UNITARI U $(U|\psi\rangle, U|\psi\rangle) = (\psi, |\psi\rangle) \rightarrow$ succede quando U è unitario

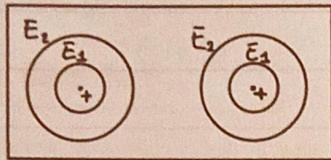
$$\Rightarrow (U^\dagger U |\psi\rangle, |\psi\rangle) = (\psi, |\psi\rangle)$$

$$U^\dagger U = I$$

$U^\dagger = \text{Trasposto coniugato}$

inverti il segno
della parte
immaginaria

PIÙ QUBITS



$$|\Psi\rangle = \alpha|E_1\rangle + \beta|E_2\rangle$$

$$|\chi\rangle = \gamma|E_1\rangle + \delta|E_2\rangle$$

$$P(E_1, E_1) = |\alpha|^2 |\gamma|^2$$

$$|\Psi\rangle = \alpha_0 |E_1\rangle |E_1\rangle + \alpha_1 |E_1\rangle |E_2\rangle + \beta_0 |E_2\rangle |E_1\rangle + \beta_1 |E_2\rangle |E_2\rangle$$

Prodotto tensoriale

$|0\rangle|0\rangle$ $|0\rangle|1\rangle$ $|1\rangle|0\rangle$ $|1\rangle|1\rangle \rightarrow$ 4 stati certi possibili (resta sovrapposizione)

Se non riesco a definirlo come prodotto (non trovo $\alpha, p, \gamma, \delta$) mi trovo in uno stato intrecciato (ENTANGLED)

$$45. |\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \stackrel{?}{=} \alpha\gamma|0\rangle|0\rangle + \alpha\delta|0\rangle|1\rangle + \beta\gamma|1\rangle|0\rangle + \beta\delta|1\rangle|1\rangle$$

$$\begin{cases} \frac{1}{\sqrt{2}} = \alpha \sigma & 0 = \alpha \delta \\ \frac{1}{\sqrt{2}} = \beta \gamma & 0 = \beta \gamma \end{cases} \rightarrow \text{non ha soluzioni}$$

Se si trovano in questo tipo di stato se separa i due atomi cosa succede?

I cosa) stato prodotto

$$\frac{1}{\sqrt{2}}(|10\rangle + |11\rangle) \quad |10\rangle = \frac{1}{\sqrt{2}}(|10\rangle|10\rangle + |11\rangle|11\rangle)$$

A E B HANNO STATISTICHE INDEPENDENTI

$B \rightarrow 10$ > independentemente da A

$$\infty \quad |\Psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle|0\rangle + |1\rangle|1\rangle)$$

$$P(10) = \frac{1}{2} \quad P(11) = \frac{1}{2}$$

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

10>10>

Se $A|0\rangle$ allora $B|0\rangle \rightarrow$ da A dipende \rightarrow

ANCHE SE
SEPARO GLI
ATOMI DI Km

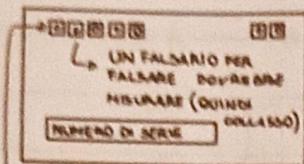
A NON RIESCE A COMUNICARE
CON B

Def

$$| \pm \rangle = \frac{1}{\sqrt{2}} (| 0 \rangle \pm | 1 \rangle) \quad \begin{cases} | + \rangle \rightarrow \theta = 45^\circ \\ | - \rangle \rightarrow \theta = 135^\circ \end{cases}$$

$$|0\rangle = \sin\theta |0\rangle + \cos\theta |1\rangle$$

QUANTUM MONEY (Banconote non contraffabbricabili)



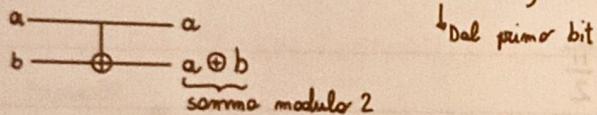
FACCIO MISURE DIVERSE IN BASE AL NUMERO DI SERIE
(NON AVVIENE IL COLLASCO PERCHÉ MISURE STATI LETTI DATI DALLA BANCA)

$$\text{Es. } \frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}} = \frac{|1\rangle|+\rangle + |-\rangle|-\rangle}{\sqrt{2}} \rightarrow \text{Verifica}$$

$$\frac{|0\rangle|1\rangle - |1\rangle|0\rangle}{\sqrt{2}} = \frac{|+\rangle|-\rangle - |-\rangle|+\rangle}{\sqrt{2}}$$

COME COSTRUIRE STATI INTRECCIATI

Porta CNOT (Porta NOT controllata)

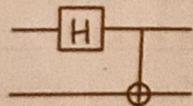


$$\text{CNOT } |\Psi\rangle = C_{00} |\Psi\rangle + C_{01} |\Psi\rangle$$

$$= C_{00} |0\rangle|0\rangle + C_{01}|0\rangle|1\rangle + C_{10}|1\rangle|0\rangle + C_{11}|1\rangle|1\rangle$$

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Entangler



$$\text{Entangler } |\Psi\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

$$|\Psi\rangle =$$

$$|\Psi\rangle =$$

$$|\Psi\rangle =$$

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

$$H|0\rangle = |+\rangle \quad H|1\rangle = |-\rangle$$

→ OTTERREMO STATI INTRECCIATI TUTTI ORTOGONALI TRA DI LORO

CODIFICA SUPERDENSNA

$$\frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

$A \rightarrow B \rightarrow$ Per mandare 2 bit classici manda 1 bit quantistico

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

Von Neumann

00 → non fa niente

01 → applica Z

10 → applica X

11 → applica iY

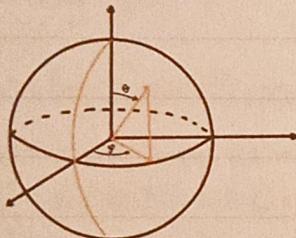
$$iY = i \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

20 Aprile lezione

IBM.com IBM quantum experience

QISIT

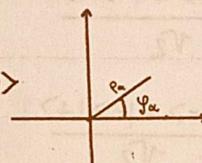
SFERA BLOCH



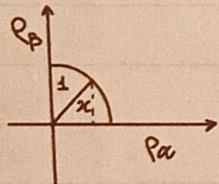
$$|\psi\rangle = \alpha|1\rangle + \beta|0\rangle$$

$$\alpha = P_\alpha e^{i\varphi_\alpha}$$

modulo e fase → posso rappresentarlo con un numero complesso



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



$$P_\alpha = \cos \chi$$

$$0 \leq \chi \leq \frac{\pi}{2}$$

$$P_\beta = \sin \chi$$

$$|\psi\rangle = P_\alpha e^{i\varphi_\alpha}|0\rangle + P_\beta e^{i\varphi_\beta}|1\rangle = e^{i\varphi_\alpha} (\cos \chi |0\rangle + \sin \chi e^{i(\varphi_\alpha + \varphi_\beta)} |1\rangle)$$

Se abbiamo una fase che moltiplica uno stato fisico la posso togliere

$$2 \chi = \theta$$

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle$$

$$\frac{|00\rangle - |11\rangle}{\sqrt{2}} =$$

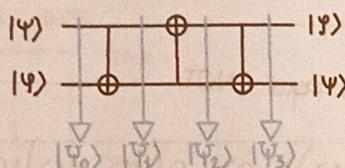
$$|++\rangle = \frac{1}{2} (|00\rangle + |11\rangle)(|00\rangle + |11\rangle) = \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

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

$$|+\rangle + |-\rangle = |00\rangle + |11\rangle$$

CIRCUITO CHE SCAMBIA 2 QUBIT (Circuito di scambio)

EXCHANGER \rightarrow 3 porte CNOT



CNOT	
$ 00\rangle$	$= 00\rangle$
$ 01\rangle$	$= 01\rangle$
$ 10\rangle$	$= 11\rangle$
$ 11\rangle$	$= 10\rangle$

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

$$|\Psi\rangle = \gamma|0\rangle + \delta|1\rangle$$

$$|\Psi_0\rangle = (\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \delta|1\rangle)$$

$$|\Psi_0\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$

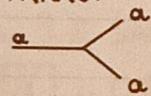
$$|\Psi_1\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|11\rangle + \beta\delta|10\rangle$$

$$|\Psi_2\rangle = \alpha\gamma|00\rangle + \alpha\delta|11\rangle + \beta\gamma|01\rangle + \beta\delta|10\rangle$$

$$|\Psi_3\rangle = \alpha\gamma|00\rangle + \alpha\delta|10\rangle + \beta\gamma|01\rangle + \beta\delta|11\rangle$$

TEOREMA DI NON CLONAZIONE

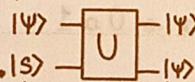
FANAUT



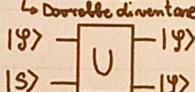
$$U^\dagger U = I$$

\rightarrow Nell'informatica classica è possibile duplicare un bit nell'informatica quantistica non è possibile creare una copia identica di uno stato quantistico sconosciuto

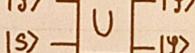
PER ASSURDO



$$|\psi\rangle \neq |\phi\rangle$$



→ corretto divenire la copia



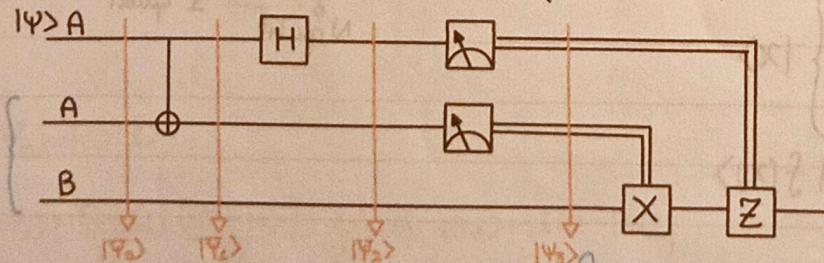
Per funzionare

$\langle \psi, \phi \rangle = 0 \rightarrow$ Funziona solo per stati ortogonali tra loro

$\langle \psi, \phi \rangle = 1$ ma $\psi \neq \phi$

Questo è dovuto alla natura dell'informazione quantistica, perché uno stato quantistico può avere le sovrapposizioni di stati, e il processo di misurazione ne altera lo stato facendolo collassare.

TELETRASPORTO QUANTISTICO (Da A a B)



MISURA
dopo ottenere
un bit
classico
"file"
quando ha un
bit classico

- QUBIT APPARTENENTI ALLO STESSO
STATO INTRECCIATO (QUELLO DI B DIVENTERÀ |ψ>

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

$$|\Psi_0\rangle = \frac{1}{\sqrt{2}} (\alpha|00\rangle + \beta|11\rangle) (|00\rangle + |11\rangle) \rightarrow |\Psi\rangle \text{ è uno stato ENTANGLED}$$

$$= \frac{1}{\sqrt{2}} (\alpha|1000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)$$

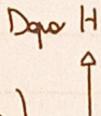
$$|\Psi_1\rangle = \frac{1}{\sqrt{2}} (\alpha|1000\rangle + \alpha|011\rangle + \beta|101\rangle + \beta|101\rangle) \rightarrow \text{Dopo CNOT}$$

$$|\Psi_2\rangle = \frac{1}{2} \left(\alpha(|0\rangle + |1\rangle)|00\rangle + \alpha(|0\rangle + |1\rangle)|11\rangle + \beta(|0\rangle - |1\rangle)|10\rangle + \beta(|0\rangle - |1\rangle)|01\rangle \right)$$

$$|\Psi_3\rangle = \frac{1}{2} \left(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle) \right)$$

Se dalla misura ottengo 00 $\rightarrow |00\rangle \underset{\text{AA}}{(\alpha|0\rangle + \beta|1\rangle)} \underset{\text{B}}{\rightarrow}$ Il qubit di B è diventato $|\Psi\rangle$

NEGLI ALTRI CASI È NECESSARIO APPLICARE DELLE PORTE PERCHÉ IL QUBIT DI B DIVENTI $|\Psi\rangle$



Non è sensibile al rumore B passate già il qubit che diventerà $|\Psi\rangle$

$$|B_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad |B_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \quad |B_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \quad |B_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

PARALLELISMO QUANTISTICO

Funzione booleana \rightarrow Ritorna solo 0 o 1

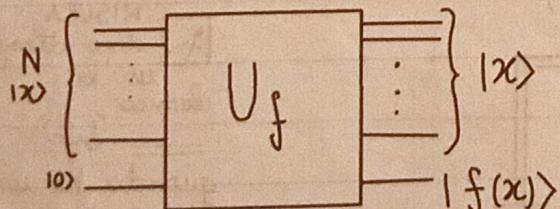
$$f(\underbrace{a_1, a_2, a_3, \dots, a_n}_{0 \leq x \leq 2^n - 1}) = \begin{cases} 0 \\ 1 \end{cases}$$

Potiamo vederla come un numero

$$U_f(|x\rangle |y\rangle) = |x\rangle |y \oplus f(x)\rangle$$

\downarrow
N qubit \downarrow
1 qubit

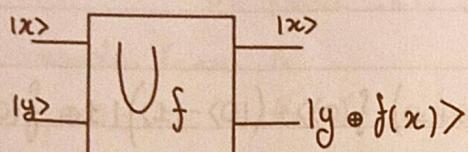
$$U_f \left(\frac{1}{\sqrt{2^N}} \sum_x |x\rangle |0\rangle \right) = \frac{1}{\sqrt{2^N}} \sum_x U_f(|x\rangle |0\rangle) = \frac{1}{\sqrt{2^N}} \sum_x |x\rangle |f(x)\rangle$$



LEZIONE 27 APRILE

Deutsch

2 QUBIT IN 2 QUBIT



funzioni booleane da un bit a un bit:

$$f(0) : \begin{matrix} 0 & 0 & 1 \end{matrix} \xrightarrow{\perp} \text{fazione '1'}$$

$$f(1) : \begin{matrix} 0 & 1 & 0 \end{matrix} \xrightarrow{\perp} \begin{matrix} 1 & 0 & 1 \end{matrix}$$

scambia QUBIT (X)

fazione "0"

fazione Identità

Da 2 bit in un bit → 16 possibilità

Se f è la funzione "0":

$$U_f = \boxed{\quad} \rightarrow \text{Due fili che non fanno nulla}$$

Se f è Identità:

$$U_f = \text{CNOT} = \boxed{\quad}$$

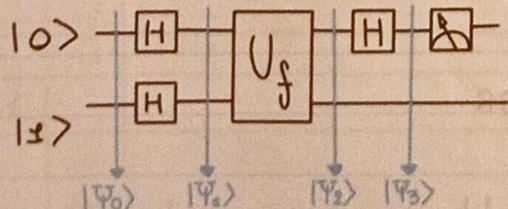
Se f è X :

$$U_f = \boxed{\quad}$$

Se f è "1"

$$U_f : \begin{aligned} |x> &\longrightarrow |x> \\ |y> &\xrightarrow{\perp} |y> \end{aligned}$$

DEUTSCH



$$|\psi_0> = |0>|1>$$

$$|\psi_1> = \frac{|0>+|1>}{\sqrt{2}} \quad |\psi_2> = \frac{|0>-|1>}{\sqrt{2}} \quad |\psi_3> = \frac{|1>+|0>}{\sqrt{2}}$$

→ CI DICE SE È COSTANTE

$$|\Psi_2\rangle = \frac{1}{2} |0\rangle |0\oplus f(0)\rangle - |0\rangle |1\oplus f(0)\rangle + |1\rangle |0\oplus f(1)\rangle - |1\rangle |1\oplus f(1)\rangle$$

$$|\Psi_3\rangle = \frac{1}{2} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) |0\oplus f(0)\rangle - (|0\rangle + |1\rangle) |1\oplus f(0)\rangle + (|0\rangle + |1\rangle) |0\oplus f(1)\rangle - (|0\rangle - |1\rangle) |1\oplus f(1)\rangle$$

caso:

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

$$|\Psi_3\rangle = \frac{1}{2} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) |f(0)\rangle - (|0\rangle + |1\rangle) |1\oplus f(0)\rangle + (|0\rangle + |1\rangle) |f(0)\rangle + (|0\rangle - |1\rangle) |1\oplus f(0)\rangle$$

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

$$f(0) \neq f(1)$$

$$f(0) = 1 \oplus f(1) \quad f(1) = 1 + f(0)$$

$$|\Psi_3\rangle = \frac{1}{\sqrt{2}} (f(0) - |1\oplus f(0)\rangle) =$$

se $|0\rangle$ è costante se $|1\rangle$ non costante

CRITTOGRAFIA

c'è un algoritmo che permette di fattorizzare in modo veloce

CRITTOGRAFIA CLASSICA BASATA SU ARITMETICA MODULARE

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

$$a = b + k \cdot n \quad n \in \mathbb{N} \quad a, b, k \in \mathbb{Z}$$

$$ux \equiv vy \pmod{n} \rightarrow \underbrace{\text{non vale } x=y \pmod{n}}_{\substack{\text{solo se } n \text{ e } u \\ \text{primi tra loro} \\ (\text{coprimi})}}$$

RSA

B vuole mandare un messaggio M

$$M = 88$$

A manda le chiavi pubbliche

$$1) A \downarrow \text{ sceglie } p, q \text{ (numeri primi molto grandi)} \quad N = p \times q$$

$$N = 187$$

$$2) e = \text{coprimo con } \underbrace{(p-1)(q-1)}_{160} \rightarrow e = 7$$

$$p=17 \quad q=11$$

3) A rende accettabile e & N

$$B \rightarrow C = M^e \pmod{N}$$

$$88^7 \pmod{187} = 11$$

B manda C ad A

• se qualcuno vuole intercettare il messaggio dovrà avere p e q di N

→ chiave di decrittazione

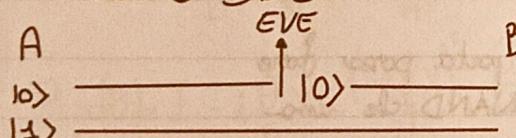
$$A \quad ed^{-1} = 1 \pmod{(p-1)(q-1)}$$

$$7d = 1 \pmod{160} \quad \longrightarrow d = 23$$

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

CRIPTOGRAFIA QUANTISTICA

PROTOCOLLO BB84



$$\begin{array}{l} \oplus \\ \otimes \end{array} \quad \begin{array}{l} 10 \rangle \circ 11 \rangle \\ 1+ \circ 1- \end{array}$$

Se usa \oplus, \otimes come base

QUESTO ALGORITMO

DICE SOLAMENTE SE

IL CANALE È SICURO

Vieno scelti casualmente una sequenza di qubit

→ va male e trova 0

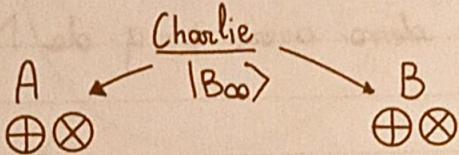
A	\oplus	\otimes	B	\oplus	\otimes
0	0	0	0	0	0
1	0	0	0	0	0
1	0	0	1	0	0

Alla fine di questo processo gli dice che hai vinto e cancella quelli che con la scelta di base sbagliate, nelle linee consigliate devono coincidere i risultati.

LEZIONE 4 MAGGIO

Ekeret (1991)

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

 $|B_{00}\rangle$ = Stato intrecciato

CIRCUITI QUANTISTICI (RISOLUTORI DI PROBLEMI)

$$\text{CNOT } \begin{array}{c} a \\ \hline b \end{array} \oplus \begin{array}{c} a \\ \hline b \end{array} = \text{NAND}$$

OR e NOT le si ottiene tramite NAND

$$\text{XOR } \Rightarrow a \oplus b = \text{NAND}(a, \text{NAND}(a, b))$$

PORTA DI TOFFOLI

$$\begin{array}{c} a \\ \hline b \\ \oplus c \end{array} \rightarrow \text{Bit di controllo}$$

con questa porta posso fare
sia una NAND che uno
FANOUT

COMPLICATITÀ

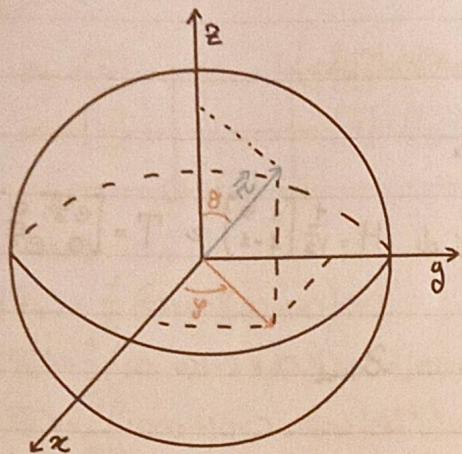
P

NP

↳ Soluzioni verificabili in un tempo
polinomiale

NP-completi

↳ Problemi che possono essere
semplificati da NP in P



$$|\Psi\rangle = \begin{bmatrix} \cos \frac{\theta}{2} \\ e^{i\phi} \sin \frac{\theta}{2} \end{bmatrix}$$

ELEVATI
AL QUADRATO
DANNO LA
MATRICE I

$$\left\{ \begin{array}{l} X = \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} \\ Y = \begin{vmatrix} 0 & i \\ i & 0 \end{vmatrix} \\ Z = \begin{vmatrix} 1 & 0 \\ 0 & -1 \end{vmatrix} \end{array} \right.$$

- $R_x(\theta) \rightarrow$ Rotazione intorno all'asse $X = e^{-i\frac{\theta}{2}}X$
 $R_y(\theta) \rightarrow$ Rotazione intorno all'asse $Y = e^{-i\frac{\theta}{2}}Y$
 $R_z(\theta) \rightarrow$ Rotazione intorno all'asse $Z = e^{-i\frac{\theta}{2}}Z$

Definiamo A e e^A :

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots + \frac{x^n}{n!} \quad n \in \mathbb{N}$$

$$R_x(\theta) = I - i\frac{\theta}{2}X + \frac{(-i\frac{\theta}{2}X)^2}{2!} + \frac{(i\frac{\theta}{2})^3 X^3}{3!} \dots$$

$$\begin{aligned} \text{sen } x &= x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} \dots \\ \text{Potenze dispari} \\ \cos x &= 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} \dots \\ \text{potenze pari} \end{aligned}$$

Dividere le potenze pari da quelle dispari

$$= I - \frac{i\theta}{2}X + \frac{-\left(\frac{\theta}{2}\right)^2 I}{2!} + \frac{i\left(\frac{\theta}{2}\right)^3 X}{3!} + \frac{\left(\frac{\theta}{2}\right)^4 I}{4!} \dots$$

$$= I \underbrace{\left(1 - \frac{\left(\frac{\theta}{2}\right)^2}{2!} + \frac{\left(\frac{\theta}{2}\right)^4}{4!} \dots\right)}_{I \cos \frac{\theta}{2}} + iX \underbrace{\left(-\frac{\theta}{2} + \frac{\left(\frac{\theta}{2}\right)^3}{3!} \dots\right)}_{-i \operatorname{sen} \frac{\theta}{2} X}$$

Le potenze pari sono moltiplicate per I ($\forall n \quad X^{2n} = I$)
 RACCOLGO $I \downarrow$

$$= \begin{bmatrix} \cos \frac{\theta}{2} & -i \operatorname{sen} \frac{\theta}{2} \\ -i \operatorname{sen} \frac{\theta}{2} & \cos \frac{\theta}{2} \end{bmatrix} \rightarrow R_x(\theta)$$

es.

$$\begin{bmatrix} \cos \frac{\theta}{2} & -i \operatorname{sen} \frac{\theta}{2} \\ -i \operatorname{sen} \frac{\theta}{2} & \cos \frac{\theta}{2} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \cos \frac{\theta}{2} \\ -\operatorname{sen} \frac{\theta}{2} \end{bmatrix}$$

TEOREMA DI UNIVERSALITÀ (Per le porte quantistiche)

1) CNOT + porta a singolo Qubit \rightarrow riesce a realizzare tutti i circuiti

2) \forall porta a ± 1 qubit, può essere approssimata con prodotti di $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ e $T = \begin{bmatrix} e^{i\pi/2} & 0 \\ 0 & e^{i\pi/2} \end{bmatrix}$

TRASFORMATA DI FURIER DISCRETA

N numeri complessi $y_0, y_1, y_2, \dots, y_{N-1} \rightarrow z_0, z_1, \dots, z_{N-1}$

$$z_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} y_j e^{2\pi i j k / N}$$

TFQ

base $|0\rangle, |1\rangle, |2\rangle, \dots, |N-1\rangle$] che sarebbe
 $|00\rangle, |01\rangle, |10\rangle$

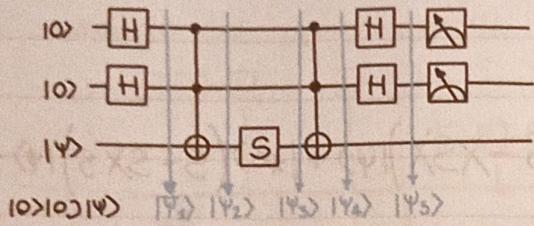
$N = 2^m \rightarrow$ m ° qubit della base

$$|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i \frac{jk}{N}} |k\rangle$$

$$J \rightarrow J_1 J_2 \dots J_m = J_1 2^{n-1} - J_2 2^{n-2} \dots J_n 2^0$$

$$0, J_1, J_2, J_3 = \frac{J_1}{2} + \frac{J^2}{2^2} + \frac{J_3}{2^3} \dots = \frac{J_1 J_2 \dots J_n}{2^n}$$

es.



$$\text{Porta di } \leftrightarrow S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

dove $S^*S = I$

Quando 1¹ la porta
di S fa il tutto
e l'altra

$$|\Psi_1\rangle = \frac{1}{2} (|00\rangle + |11\rangle)(|00\rangle + |11\rangle)|\psi\rangle$$

$$|\Psi_2\rangle = \frac{1}{2} (|00\rangle |\psi\rangle + |01\rangle |\psi\rangle + |10\rangle |\psi\rangle + |11\rangle X|\psi\rangle)$$

$$|\Psi_3\rangle = \frac{1}{2} ((|00\rangle + |01\rangle + |10\rangle)S|\psi\rangle + |11\rangle SX|\psi\rangle) \text{ si apre sull'ultimo QUBIT}$$

$$|\Psi_4\rangle = \frac{1}{2} ((|00\rangle + |01\rangle + |10\rangle)S|\psi\rangle + |11\rangle XS|\psi\rangle)$$

$$|\Psi_5\rangle = \frac{1}{4} \left[[(|00\rangle + |11\rangle)(|0\rangle + |1\rangle) + (|0\rangle + |1\rangle)(|0\rangle + |1\rangle) + (|0\rangle - |1\rangle)(|0\rangle + |1\rangle)] S|\psi\rangle + (|0\rangle - |1\rangle) \right. \\ \left. (|0\rangle - |1\rangle)XS|\psi\rangle \right]$$

$$|\Psi_5\rangle = \frac{1}{4} \left[|00\rangle (3S + XSX)|\psi\rangle + |01\rangle (S - XSX)|\psi\rangle + |10\rangle (S - SXS)|\psi\rangle + \right. \\ \left. + |11\rangle (-S + XSX)|\psi\rangle \right] \rightarrow \text{Dividiamo per la norma per ottenere stati normalizzati}$$

$$3S + XSX = \begin{pmatrix} 3 & 0 \\ 0 & 3i \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & 3i \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 3+i & 0 \\ 0 & 3i+1 \end{pmatrix}$$

$$= 3+i \begin{pmatrix} 1 & 0 \\ 0 & \frac{3i+1}{3+i} \end{pmatrix} = 3+i \begin{pmatrix} 1 & 0 \\ 0 & \frac{(3+i)(3-i)}{10} \end{pmatrix} = 3+i \begin{pmatrix} 1 & 0 \\ 0 & \frac{8i+6}{10} \end{pmatrix} = 3+i \begin{pmatrix} 1 & 0 \\ 0 & \frac{3+i}{5} \end{pmatrix}$$

$$\left((3+i) \begin{pmatrix} 1 & 0 \\ 0 & \frac{3+i}{5} \end{pmatrix} |\psi\rangle, (3+i) \begin{pmatrix} 1 & 0 \\ 0 & \frac{3+i}{5} \end{pmatrix} \frac{1}{5} |\psi\rangle \right) = \\ = \left(|\psi\rangle, (3+i) \begin{pmatrix} 1 & 0 \\ 0 & \frac{3-i}{5} \end{pmatrix} (3+i) \begin{pmatrix} 1 & 0 \\ 0 & \frac{3+i}{5} \end{pmatrix} \right)$$

$$= 20 \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{5} \end{pmatrix}$$

$$P(00) = \left(\frac{1}{4} \cdot \frac{1}{\sqrt{10}}\right)^2 = \frac{5}{8}$$

$$|\Psi_5\rangle = \frac{1}{4} \left[\frac{|\text{H}\rangle|0\rangle (3S+XSX)|\psi\rangle + |\text{D}\rangle (S-XSX)|\psi\rangle + |\text{D}\rangle (S-SXS)|\psi\rangle + |\text{D}\rangle (-S+XSX)|\psi\rangle }{\sqrt{10}} \right]$$

$$S - XSX = (1-i) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

NEL CASO IO CON LA MISURA OTTENGO DO COLASSA

SU $\frac{(3S+XSX)|\psi\rangle}{\sqrt{10}}$ E UNA ROTAZIONE $\begin{pmatrix} 4 & 0 \\ 0 & \frac{3+i}{5} \end{pmatrix}$

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \cos \theta = \frac{3}{5} \quad \sin \theta = \frac{4}{5} = R_Z(\theta) = e^{-i\frac{\theta}{2}Z}$$

TRASFORMATA DI FOURIER DISCRETA (QUANTISTICA) TFOQ

$|1000\rangle, |1000-1\rangle, \dots, |1111\rangle$ BASE $\nwarrow N = 2^n$

TFQ su $|j_1 \dots j_n\rangle \equiv \frac{1}{2^{\frac{n}{2}}} \sum_{k=0}^{2^n-1} e^{2\pi i \frac{j_k}{2^n} k} |k\rangle$ $\begin{array}{l} \text{vettori base} \\ \text{individuati da} \\ \text{una linea di} \\ \text{base} \end{array}$ $= \frac{1}{2^{\frac{n}{2}}} \sum_{k_1=0}^1 \sum_{k_2=0}^1 \dots \sum_{k_n=0}^1 e^{2\pi i \frac{j_k}{2^n} (k_1 2^{n-1} + \dots + k_n 2^0)}$

$$= \frac{1}{2^{\frac{n}{2}}} \sum_{k_1=0}^1 \sum_{k_2=0}^1 e^{2\pi i \frac{j}{2^n} k_1 2^{n-1}} \dots e^{2\pi i \frac{j}{2^n} k_n 2^0} |k_1\rangle |k_2\rangle \dots |k_n\rangle$$

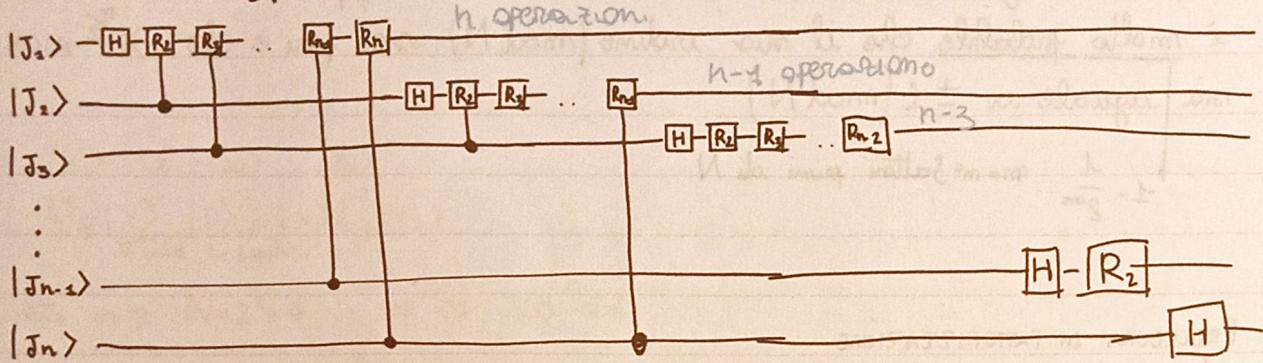
$$= \frac{1}{2^{\frac{n}{2}}} \sum_{k_1=0}^1 e^{2\pi i \frac{j}{2} k_1} |k_1\rangle \dots \sum_{k_n=0}^1 e^{2\pi i \frac{j}{2^n} k_n} |k_n\rangle$$

$$= \frac{1}{2^{\frac{n}{2}}} \left(|0\rangle + e^{2\pi i \frac{j}{2}} |1\rangle \right) \dots \left(|0\rangle + e^{2\pi i \frac{j}{2^n}} |1\rangle \right)$$

\downarrow
se $k_1=0$ $k_1=1$ $\frac{j_n}{2}$

$$= \frac{1}{2^{\frac{n}{2}}} \left(|0\rangle + e^{2\pi i \frac{j}{2} \cdot 0 \cdot j_n} \right) \dots \left(|0\rangle + e^{2\pi i \frac{j}{2^n} \cdot 0 \cdot j_1 \cdot j_2 \dots j_n} |1\rangle \right)$$

CIRCUITO CHE LA IMPLEMENTA



$$R_R = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i / 2^k} \end{pmatrix}$$

$$n + (n-1) + (n-2) \dots = \frac{m(m+1)}{2}$$

crece n^2

$m 2^m \rightarrow$ NEL CALCOLATORI
NON QUANTISTICI

Ricerca dell'ordine

ORDINE (+ un piccolo intero)

$$x^n \equiv 1 \pmod{N}$$

ESISTE SEMPRE SE x e N sono coprimi

es.

$$4^n \equiv 1 \pmod{91} \quad n=6 \quad 4^6 = 4096 = 1 + 45 \times 91$$

algoritmo che
trova n

Fattorizzazione

In: se N è composito (non primo) e \rightarrow Escludere le soluzioni banali ($1 < y < N-1$)

y è una soluzione $y^2 \equiv 1 \pmod{N}$

$$\Rightarrow \begin{cases} \text{MCD}(y-1, N) \\ \text{MCD}(y+1, N) \end{cases}$$

sono fattori non banali di N

Dim:

$$y^2 \equiv 1 \pmod{N} \Rightarrow y^2 - 1 \equiv 0 \pmod{N}$$

$$N \text{ divide } y^2 - 1 = (y+1)(y-1)$$

$$N > y-1 > y+1$$

$$\text{Piplo} = \frac{y^2 - 1}{N}$$

FATTORI NON BANALI DI N

Facili da trovare se trovi y

Th²: Se si sceglie a caso un intero $X \quad 1 \leq X \leq N-1$, coprimo con N allora è molto probabile che il suo ordine $(\text{mod } N)$ sia pari e che $X^{\frac{n}{2}}$ non sia uguale a $\pm 1 \pmod{N}$

$$1 - \frac{1}{2^m} \quad m = \text{n. fattori primi di } N$$

PROCEDURA DI FATTORIZZAZIONE

$$O((\log_2 N)^2) \rightarrow \text{compl.}$$

INPUT: N

OUTPUT: Un fattore non banale di N

1. Se N è pari output: 2

2. Determinare se $N = a^b$ output: a

es. 91 (no paro 1 e 2)

3. X tra 1 e $90 \quad X \cdot 4 \rightarrow$ a caso tra quelli coprimi con 91

3. scegliere X tra $[1, N-1]$

calcola M.C.D. (x, N) se $\text{MCD}(x, N) > 1$ output: MCD

4. Ricerca ordine $r \rightarrow X^r \equiv \pm 1 \pmod{N}$

5. Se r è pari e $X^{\frac{r}{2}} \neq \pm 1 \pmod{N}$
 $\Rightarrow \text{MCD}(X^{\frac{r}{2}} \pm 1, N) \rightarrow$ output: MCD

RICERCA IN UN DATABASE

$N \rightarrow$ elementi nel DB

Algoritmo di Grover

problema: trovare in un database soli $N = 2^n$ elementi, in un sottoinsieme di soli M elementi che soddisfano una condizione data

M soluzioni.

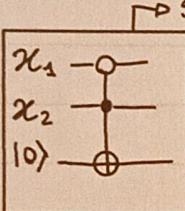
- Si suppono che $\exists f$ che mi dice se un elemento è una soluzione
 \hookrightarrow BOOLEANA

- $|X\rangle = |x_1\rangle |x_2\rangle \dots |x_n\rangle$

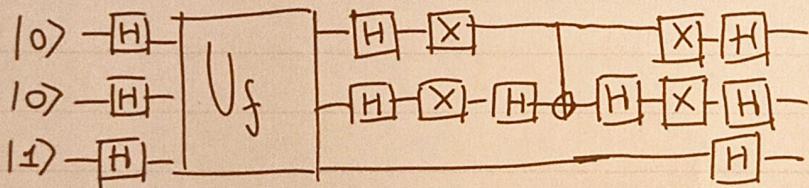
$$U_f |X\rangle |0\rangle = |X\rangle |f(x)\rangle$$

$\underbrace{\qquad\qquad\qquad}_{m \text{ qubit}}$ $\underbrace{\qquad\qquad\qquad}_{\hookrightarrow 1 \text{ qubit}}$

es. $m:2 \quad N=2^2=4$ 00 01 10 11

$U_f =$ 

\hookrightarrow so che esiste
U_f ma non so
come farla



Il guadagno è di ordine quadratico $\Theta(\sqrt{N}) = \Theta(1/2^n)$
 al posto di $\Theta(N)$ con l'informatica classica