Curs 7 STLS II

→ un sistem format din n qubiți

$H_2 \otimes H_2 \otimes \dots \otimes H_2$ $\qquad H_2 = \left(\mathbb{C}^2, \sum_{i=1}^{2} x_i \bar{y}_i\right)$

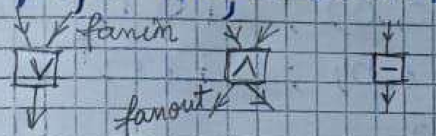
Baza $\{ |x_1\rangle |x_2\rangle \dots |x_n\rangle \mid x_i \in \{0,1\}\}$ $\qquad$ dim $= 2^n$

are 2^n elemente; "registru cuantic de lungime n".

Starea registrului: $c_0|0\rangle + c_1|1\rangle + \dots + c_{2^n-1}|2^n-1\rangle$

cu condiția $|c_0|^2 + |c_1|^2 + \dots + |c_{2^n-1}|^2 = 1$

superpoziția conține 2^n-1 numere complexe.



porți logice

→ poarta cuantică unară $\qquad U: H_2 \to H_2$

$|0\rangle \to a|0\rangle + b|1\rangle$ $\qquad$ matrice unitară $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$|1\rangle \to c|0\rangle + d|1\rangle$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad A^* = \underbrace{\bar{A}^T}_{\text{A transpus conjugat}} = A^{-1}$$

~~Exemple~~: ① $M_\neg = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\qquad |0\rangle \to |1\rangle$, $\quad |1\rangle \to |0\rangle$

matr. negației

② $$\sqrt{M_\neg} = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}$$

$$\sqrt{M_\neg}^* = \begin{pmatrix} \frac{1-i}{2} & \frac{1+i}{2} \\ \frac{1+i}{2} & \frac{1-i}{2} \end{pmatrix}$$

$\sqrt{M_\neg}\,\sqrt{M_\neg}^* \overset{\text{calcule}}{=} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = id$

unitară.

$$\sqrt{M_\Gamma}^{\,2} \overset{\text{calcule}}{=} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$ „$\sqrt{NU}$"

(3) $$W_2 = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}$$ Hadamard Walsh „$\sqrt{DA}$"

→ porți cuantice binare $U : H_4 \to H_4$

convenție notare
$|00\rangle^T = (1,0,0,0)$; $|01\rangle^T = (0,1,0,0)$
$|10\rangle^T = (0,0,1,0)$; $|11\rangle^T = (0,0,0,1)$

Negația condiționată (controlată)

$$M_{Cnot} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$M_{Cnot} |x_0 x_1\rangle = |x_0, x_0 \oplus x_1\rangle$$

$$M^*_{Cnot} = M_{Cnot}$$

$M_{Cnot} \cdot \underbrace{M_{Cnot} = id}_{\text{rămâne de verificat}} \Rightarrow M_{Cnot}$ unitară (ca să iasă)

↙ se obs. din calcule -- q.e.d.

Produsul tensorial de aplicații liniare (produsul Kroneker)

A matrice $r \times s$ B matrice $t \times u$

~~prod Kroneker~~ $A = \begin{pmatrix} a_{11} & \cdots & a_{1s} \\ \vdots & & \vdots \\ a_{r1} & \cdots & a_{rs} \end{pmatrix}$

prod. Kroneker :

prod. Kroneker: $A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1s}B \\ a_{21}B & a_{22}B & \cdots & a_{2s}B \\ \hline a_{k1}B & a_{k2}B & \cdots & a_{ks}B \end{pmatrix}$

$M_1 : H_n \to H_n$
$M_2 : H_m \to H_m$ | $M_1 \otimes M_2 : H_n \otimes H_m \to H_n \otimes H_m$

prod. tensorial nu produce entaglement.

Exemplu $M_1 = M_2 = W_2$ Hadamard Walsh

$$W_4 = W_2 \otimes W_2 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \qquad W_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Obs. element al bazei lui H_4

$$W_4 |x_0 x_1\rangle = \frac{1}{2}\left(|0\rangle + (-1)^{x_0}|1\rangle\right) \otimes \left(|0\rangle + (-1)^{x_1}|1\rangle\right) =$$

$$= \frac{1}{2}\left(|00\rangle + (-1)^{x_0}|01\rangle + (-1)^{x_1}|10\rangle + (-1)^{x_0+x_1}|11\rangle\right).$$

decompozabilă! W_4 nu produce entanglement

Obs. M_{cnot} nu este produs tensorial de matrice.

$$S = (W_2 \otimes I_2)|00\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle =$$

$$= \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \to S \text{ decompozabilă}$$

$$M_{cnot} S = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad \text{EPR indecompozabilă}$$

M_{cnot} nu este decompozabilă ca produs tensorial.

Th de neclonare (Wooters și Zurek)

$|a_1\rangle, \dots, |a_n\rangle$, H_n, $|a_1\rangle$ blank.

$U : H_n \otimes H_n \to H_n \otimes H_n$

$\forall |x\rangle \in H_n$ $\cancel{\exists}$ $U(|x\rangle|a_1\rangle) = |x\rangle|x\rangle$

„mașină cuantică de copiat".

Dacă $n>1$, atunci $\nexists$ nicio mașină cuantică de copiat.

Dem

$n>1 \Rightarrow \exists$ cel puțin două stări pure $|a_1\rangle$ și $|a_2\rangle$ ortogonale.

$$U(|a_1\rangle|a_1\rangle) = |a_1\rangle|a_1\rangle$$

$$U(|a_2\rangle|a_1\rangle) = |a_2\rangle|a_2\rangle$$

$$U\Big(\overbrace{\tfrac{1}{\sqrt2}(|a_1\rangle+|a_2\rangle)}^{x}|a_1\rangle\Big) = U\Big(\tfrac{1}{\sqrt2}(|a_1\rangle|a_1\rangle+|a_2\rangle|a_1\rangle)\Big)$$

$$= \tfrac{1}{\sqrt2}|a_1\rangle|a_1\rangle + \tfrac{1}{\sqrt2}|a_2\rangle|a_2\rangle$$ entangled

abs

pe de altă parte

$$= \tfrac{1}{\sqrt2}(|a_1\rangle+|a_2\rangle)\,\tfrac{1}{\sqrt2}(|a_1\rangle+|a_2\rangle)$$ decompozabil

În lumea cuantică, orice proces studiat până acum este reversibil, spre deosebire de lumea macroscopică.

$A = \mathbb{F}_2$ $\{\vee, \wedge, \neg\}$ familie completă de funcții

$\Updownarrow$

$\forall f: \mathbb{F}_2^n \to \mathbb{F}_2^m$ se poate scrie ca tuplu de expresii booleene.

Circuitul boolean: graf aciclic orientat

x_i variabile de intrare

y_j variabile de ieșire

$\wedge, \vee$ fanin $=2$, fanout ≥ 1

$\neg$ fanin $=1$, fanout ≥ 1

O operație (poartă) ~~de~~ reversibilă: $f: \mathbb{F}_2^n \to \mathbb{F}_2^n$ bijectivă

Exemple: ① Poarta Toffoli

$$T(x_1, x_2, x_3) = (x_1, x_2, x_1 x_2 + x_3)$$

$$\mathbb{F}_2^3 \to \mathbb{F}_2^3$$

② Negația controlată $N: \mathbb{F}_2^2 \to \mathbb{F}_2^2$

$$N(x_1, x_2) = (x_1, x_1 + x_2)$$

<u>Circuit reversibil</u>: permutare a lui $\mathbb{F}_2^n$ compusă din operații reversibile.

$C: \mathbb{F}_2^n \to \mathbb{F}_2^n$

• dacă $C(x_1, \dots, x_n)$ este o funcție booleană oarecare, atunci $\exists f: \mathbb{F}_2^{n+m} \to \mathbb{F}_2^{n+m}$ reversibilă și $\exists c_1, \dots, c_m \in \mathbb{F}_2$ constante ~~$d_1, \dots, d_m$~~ a.î.

$\forall x_1, \dots, x_n \in \mathbb{F}_2$, $f(x_1, \dots, x_n, c_1, \dots, c_m) =$

$= (C(x_1, \dots, x_n), d_1, \dots, d_m)$ ⇝ Orice fcț. se poate ascunde în una reversibilă.

Lemă $\{\neg, N, T\}$ = mulțime universală, necesită doar constanta 0.

(negație, negație controlată, poarta Toffoli)

<u>Dem.</u> • negația e reversibilă, o folosim direct

• $T(x_1, x_2, 0) = (x_1, x_2, x_1 x_2) \Rightarrow$ putem calcula $\wedge$

• $x_1 \vee x_2 = \neg(\neg x_1 \wedge \neg x_2) \Rightarrow$ putem calcula $\vee$ (de Morgan)

• $N(x_0, 0) = (x_0, x_0) \Rightarrow$ putem simula porți cu fanout > 1.

Th Poarta Toffoli este poartă reversibilă universală

<u>Dem.</u> $T(1, 1, x) = (1, 1, \neg x) \to \neg$

$T(1, x, y) = (1, x, x + y) \to N$ $\square$

$\vec{x} \in \mathbb{F}_2^m \xrightarrow{\text{identif.}} |\vec{x}\rangle = e_i = (0, 0, \dots, 0, \underset{\text{poz. } i}{1}, 0, \dots, 0, 0)^T$

unde $\vec{x}$ = reprezentarea binară a lui $i+1$.

$$T = \begin{pmatrix} I_2 & 0 & 0 & 0 \\ 0 & I_2 & 0 & 0 \\ 0 & 0 & I_2 & 0 \\ 0 & 0 & 0 & M_\neg \end{pmatrix}$$

8×8 poarta Toffoli

modifică stringul $x_0 x_1 x_2$ numai în cazurile:

$110 \rightsquigarrow 111$

și

$111 \rightsquigarrow 110$ i.e.

i.e. $e_7 \rightsquigarrow e_8$ și $e_8 \rightsquigarrow e_7$

Fie G grup finit, P probabilitatea evenimentului

$C = \{ (x,y) \in G \times G \mid xy = yx \}$.

Th) Dacă $P = \overset{prob}{P}(C) > \frac{5}{8} \Rightarrow G$ abelian

Dem: Fie centrul grupului $Z(G) = \{ x \in G \mid \forall y \; xy = yx \}$

$1 \triangleleft_G$ subgrup normal

Obs:
- $|G : Z(G)| = 1 \Rightarrow G = Z(G) \Rightarrow$ grup abelian
- $|G : Z(G)| = 2 \Rightarrow \exists u \; \forall x \notin Z(G) \Rightarrow \exists y \in Z(G)$ cu $x = uy$

Deci $G = \langle Z(G), u \rangle$ (generat de centru și un singur elem. unic) $\Rightarrow G$ abelian

- $|G : Z(G)| = 3 \Rightarrow G = Z(G) \cup aZ(G) \cup a^2 Z(G)$

Deci $G = \langle Z(G), a \rangle \Rightarrow G$ abelian

- $|G : Z(G)| = 4 \Rightarrow$ fie $G/Z(G) \overset{abelian}{\simeq} \mathbb{Z}_4$,

fie $\underbrace{G/Z(G) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2}_{\text{ar putea să nu fie abelian}}$

$G = \{ \pm 1, \pm i, \pm j, \pm k \}$

$ij = k, \; jk = i, \; kj = j$

$ji = -k, \; kj = -i, \ldots \quad i^2 = j^2 = k^2 = -1$

unitățile corpului quaternionilor necomutativ

$Z(G) = \{ \pm 1 \} \qquad G/Z(G) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$

$g \in G \setminus Z(G) \Rightarrow |G : C(g)| \geq 2$

centralizatorul lui g $\quad C(g) = \{ x \in G \mid xg = gx \} \trianglelefteq G$

- $|G : C(g)| = 1 \Rightarrow g \in Z(G)$ $\not\!\!\!\times$
- $|G : C(g)| = 2$ de exemplu $C(i) = \{ \pm 1, \pm i \}$

G nu e abelian, $(x,y) \in G \times G$

- cu prob. $\leq \frac{1}{4}$, x comută cu toate elementele
- cu prob. $\geq \frac{3}{4}$, x comută cu $\leq \frac{1}{2}$ elemente

$$P(xy = yx) \leq \frac{1}{4} \cdot 1 + \frac{3}{4} \cdot \frac{1}{2} = \frac{5}{8}.$$

cercul complex $\quad C = \{ (z_1, z_2) \in \mathbb{C}^2 \mid z_1^2 + z_2^2 = 1 \}$ dim. complexă 1, dim. reală 2

sfera qubiților $\quad Q = \{ (z_1, z_2) \in \mathbb{C}^2 \mid |z_1|^2 + |z_2|^2 = 1 \}$ dim. reală 3, nu are dim. complexă

$$C: \ (x_1 + i y_1)^2 + (x_2 + i y_2)^2 = 1 \iff$$

$$\iff \begin{cases} 1 + y_1^2 + y_2^2 = x_1^2 + x_2^2 \ (*) \\ x_1 y_1 + x_2 y_2 = 0 \end{cases}$$

$$Q: \quad x_1^2 + x_2^2 + y_1^2 + y_2^2 = 1$$

$$\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right) \in Q \setminus C \qquad (i, \sqrt{2}) \in C \setminus Q$$

$x_1 = 0 \quad x_2 = \sqrt{2}$

$y_1 = 1 \quad y_2 = 0$

$$Q \cap C = ?$$

$$\begin{cases} 1 + y_1^2 + y_2^2 + y_1^2 + y_2^2 = 1 \\ x_1 y_1 + x_2 y_2 = 0 \end{cases}$$

$$\boxed{y_1^2 + y_2^2 = 0} \qquad \boxed{y_1 = y_2 = 0} \Rightarrow \text{din } (*) \ x_1^2 + x_2^2 = 1$$

$$(x_1, x_2, y_1, y_2) = (\sin\theta, \cos\theta, 0, 0)$$

Deci $Q \cap C$ = cerc real de dimensiune 1.