

# Special Topics in Security and Applied Logic

2 - Curs 7 - 06.04.2023

Un sistem format din  $n$  qubituri.

$$dim = 2^m$$

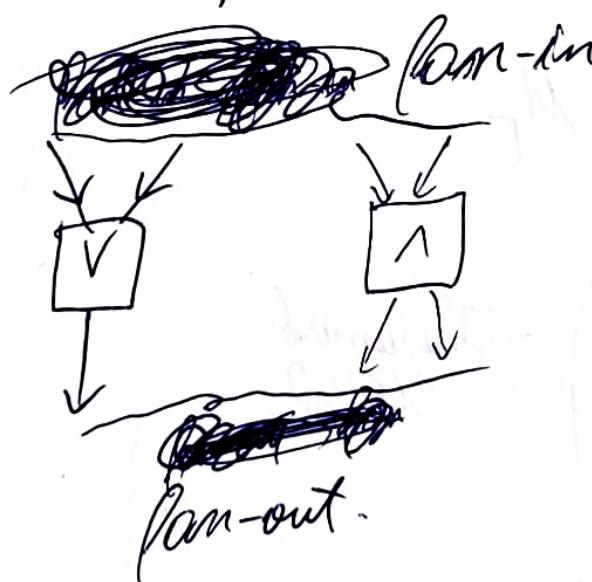
$$H_1 \otimes H_2 \otimes \dots \otimes H_n, H_n = \left( \mathbb{C}^2, \sum_{i=1}^2 x_i |i\rangle \right)$$

- Baza  $\{|x_1\rangle |x_2\rangle \dots |x_m\rangle |x_i \in \{0,1\}\}$ ,  $2^n$ -elemente; "registru cuantic de lungime  $m$ "

O stare a registruului:  $C_0 |0\rangle + C_1 |1\rangle + \dots + C_{2^m-1} |2^m-1\rangle$

$$\text{cu conditia } |C_0|^2 + |C_1|^2 + \dots + |C_{2^m-1}|^2 = 1$$

- Aceasta superpozitie contine  $2^m-1$  numere complexe



Porta cuantica unitara:  $U: H_2 \rightarrow H_2$

$$|0\rangle \rightarrow a|0\rangle + b|1\rangle$$

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

a-i. Matricea extinsa este

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\text{adica } A^{-1} := (A^\dagger)^{-1} = \frac{1}{\sqrt{5T3AL2}} \quad \boxed{7.1}$$

Exemplu: ① "Matricea negativă":

$$M_F = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \begin{matrix} |0\rangle \rightarrow |1\rangle \\ |1\rangle \rightarrow |0\rangle \end{matrix}$$

② "Produsul patrata al negativi":

$$\sqrt{M_F} = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix} \quad \text{"VNU"}$$

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

$$\sqrt{M_F} \cdot \sqrt{M_F}^* = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 \Rightarrow \text{Matricea e unitară}$$

$$\sqrt{M_F}^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = M_F$$

$$③ W_2 = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \quad \text{- Hadamard Matrix}$$

"VDA"

Portii cuantice binare:  $U: H_4 \rightarrow H_4$

~~100~~  $|00\rangle^T = (1, 0, 0, 0)$ ;  $|01\rangle^T = (0, 1, 0, 0)$ ;  
 $|10\rangle^T = (0, 0, 1, 0)$ ;  $|11\rangle^T = (0, 0, 0, 1)$ ;

# Ologica condizionale / controllata:

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

$$M_{cnot} \cdot |X_0 X_1\rangle = |X_0, X_0 \oplus X_1\rangle$$

$$M_{cnot}^* = M_{cnot}$$

$$M_{cnot} \cdot M_{cnot} = i\mathbb{I} \Rightarrow M_{cnot} \text{ e unitaria}$$

Prodotto Kronecker / ~~prodotto~~ entre matrice ~~matrice~~  
~~tensoriale~~

Se A è matrice  $n \times p$   
B - matrice  $t \times u$

$$A = \begin{pmatrix} a_{11} & \dots & a_{1p} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{np} \end{pmatrix}$$

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1p}B \\ \vdots & & & \vdots \\ a_{n1}B & a_{n2}B & \dots & a_{np}B \end{pmatrix}$$

tensor bloc matrice

Se  $M_1: H_m \rightarrow H_m$ , otteni  $M_1 \otimes M_2: H_m \otimes H_m \rightarrow H_m \otimes H_m$

$M_2: H_m \rightarrow H_m$

Quest prodotto tensoriale  
non produce entanglement

Exemplu:

$$\text{Fie } M_1 = M_2 = W_2 \text{ (Hadamard Walsh)} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

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

(Obs.:

dimensiunea lui  $H_4$

$$W_4 |X_0 X_1\rangle = \frac{1}{2} (|0\rangle + (-1)^{X_0} |1\rangle) \otimes (|0\rangle + (-1)^{X_1} |1\rangle) =$$

$$= \frac{1}{2} (|00\rangle + (-1)^{X_0} |01\rangle + (-1)^{X_1} |10\rangle + (-1)^{X_0+X_1} |11\rangle)$$

Deci e decompozabilă!  $W_4$  nu produce entanglement.

(Obs.:

$M_{\text{cnot}}$  nu este produs tensorial de matrice

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

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

$S$  - decompozabilă.

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

(Entanglement, ...)

care e indecompozabilă.  $\Rightarrow$

$\Rightarrow M_{\text{cnot}}$  nu e decompozabilă ca produs tensorial

## Teorema de nedonare (Wooters și Zurek)

Este un sistem cu basă  $|a_1\rangle, \dots, |a_n\rangle$   
 $H_m, \quad \text{[del] } |a_1\rangle \text{ blank.}$

$$U: H_m \otimes H_m \rightarrow H_m \otimes H_m.$$

$\forall |x\rangle \in H_m, \quad U(|x\rangle |a_1\rangle) = |x\rangle |x\rangle$   
 "monstru cuantic de copiat"

①: Dacă  $n > 1$ , atunci nu există nicio matrice  
 cuantică de copiat.

Dem.:  $n > 1 \Rightarrow$  există cel puțin 2 stări pure  $|a_1\rangle, |a_2\rangle$   
 și ortogonale

$$\text{ipoteză} \Rightarrow U(|a_1\rangle |a_1\rangle) = |a_1\rangle |a_1\rangle$$

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

$$U\left(\underbrace{\frac{1}{\sqrt{2}}(|a_1\rangle + |a_2\rangle)}_{X} |a_1\rangle\right) \stackrel{\text{①}}{=} U\left(\frac{1}{\sqrt{2}}(|a_1\rangle |a_2\rangle + |a_2\rangle |a_1\rangle)\right) =$$

$$= \frac{1}{\sqrt{2}}|a_1\rangle |a_1\rangle + \frac{1}{\sqrt{2}}|a_2\rangle |a_2\rangle \quad \leftarrow \text{entangled.}$$

$$\text{② } \frac{1}{\sqrt{2}}(|a_1\rangle + |a_2\rangle) \cdot \frac{1}{\sqrt{2}}(|a_1\rangle + |a_2\rangle) \quad \leftarrow \text{decompozabil}$$

$\Rightarrow X$

$\exists$   $A = F_2^m$

Stim ca  $2V, 1, \Gamma$  formeaza o familie completa de functii:

$\forall f: F_2^n \rightarrow F_2^m$  se poate scrie ca un tuplu de expresii booleene.

Circuit boolean: Graf aciclic orientat

$x_i$  - variabile de intrare

$y_j$  - variabile de ieșire

$N, V$  -  $\begin{cases} \text{fan-in} = 2 \\ \text{fan-out} \geq 1 \end{cases}$

$\Gamma$  -  $\begin{cases} \text{fan-in} = 1 \\ \text{fan-out} \geq 1 \end{cases}$

O operatie/poarta reversibila este ~~o~~ o

$f: F_2^m \rightarrow F_2^m$

bijectiva

Exemplu 1: Poarta Toffoli

$$T(x_1, x_2, x_3) = (x_1, x_2, \cancel{x_3}, x_1x_2 + x_3)$$

$$F_2^3 \rightarrow F_2^3$$

Ex 2: Negativa controlata

$$N: F_2^2 \rightarrow F_2^2, N(x_1, x_2) = (x_1, x_1 + x_2)$$

Circuit reversibil: permutare a lui  $\mathbb{F}_2^n$  compusa din operatii reversibile.

\* Daca  $C(\bar{x}_1, \dots, \bar{x}_n)$  este o functie booleana oarecare  $\Rightarrow \exists f: \mathbb{F}_2^{n+m} \rightarrow \mathbb{F}_2^{n+m}$  cu  $c_1, \dots, c_m \in \mathbb{F}_2$  constante a.t.

$$\forall \bar{x}_1, \dots, \bar{x}_n \in \mathbb{F}_2, f(\bar{x}_1, \dots, \bar{x}_n, c_1, \dots, c_m) = \\ = (C(\bar{x}_1, \dots, \bar{x}_n), d_1, \dots, d_m)$$

Lemă:  $\{T, N, T\}$  - multime universala, recentata doar constanta 0.

Dem.: • negatie & reversibilitatea poate fi folosita direct

• Observam ca  $T(x_1, x_2, 0) = (x_1, x_2, x_1 x_2) \Rightarrow$   
⇒ putem calcula conjunctia.

•  $x_1 \vee x_2 = \cancel{(x_1 \vee x_2)} \rightarrow (\neg x_1 \wedge \neg x_2) \Rightarrow$  putem calcula disjunctia.

•  $N(x_0, 0) = (x_0, x_0) \Rightarrow$  putem formula porti cu fan-out  $> 1$

( $\textcircled{T}$ ) Poarta Toffoli este poarta reversibila universala.

Dem.:  $T(1, 1, X) = (1, 1, \bar{X}) \Rightarrow$  se poate obtine  $\neg$

$T(1, X, 1) = (1, X, X + 1) \Rightarrow$  se poate obtine  $N$

□

$\vec{x} \in F_2^m$  identic,  $|\vec{x}\rangle = l_i = (0, 0, \dots, \overset{i}{1}, 0, \dots, 0)^T$

unde  $\vec{x}$  reprezintă rea binară a lui  $i+1$

$$T_{(8 \times 8)} = \begin{pmatrix} I_2 & 0 & 0 & 0 \\ 0 & I_2 & 0 & 0 \\ 0 & 0 & I_2 & 0 \\ 0 & 0 & 0 & M_T \end{pmatrix}$$

Modifică stringul  $x_0x_1x_2$  numai în carurile

$$\begin{array}{l} 110 \rightsquigarrow 111 \text{ adică } l_4 \rightsquigarrow l_8 \\ 111 \rightsquigarrow 110 \text{ adică } l_8 \rightsquigarrow l_7 \end{array}$$

Eserciziu:

Este 5-grup finit.  $P$ -probabilitatea evenimentului

$$C = \{(x, y) \in 5 \times 5 \mid x+y = yx\}$$

(T) Dacă  $P = P(C) > \frac{5}{8} \Rightarrow 5$  e abelian

Dem.: Este central grupului  $Z(5) =$

$$= \{x \in 5 \mid x+y = yx\} \trianglelefteq 5$$

(subgrup normal)

Dacă  $|5 : Z(5)| = 1 \Rightarrow 5 = Z(5) = 0$  5-abelian

$$\bullet |5 : Z(5)| = 2 \Rightarrow \exists u, x \in 5 \setminus Z(5) \Rightarrow$$

(induce 2)

$$\Rightarrow \forall v \in Z(5) \text{ și } x = uv / \overline{\text{ST 5 AL 2. c}} \quad \overline{7 \cdot 8}$$

$\Rightarrow \mathbb{F} = \langle \mathbb{Z}(6), u \rangle \Rightarrow \mathbb{F}$ -abelian.

- $|\mathbb{F} : \mathbb{Z}(6)| = 3 \Rightarrow \mathbb{F} = \mathbb{Z}(6) \cup a \cdot \mathbb{Z}(6) \cup a^2 \cdot \mathbb{Z}(6)$   
 $\Rightarrow \mathbb{F} = \langle \mathbb{Z}(6), a \rangle \Rightarrow \mathbb{F}$ -abelian.

- $|\mathbb{F} : \mathbb{Z}(6)| = 4 \Rightarrow \text{nu } \mathbb{F}/\mathbb{Z}(6) \cong \mathbb{Z}_4$  sau  $\mathbb{F}/\mathbb{Z}(6) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$   
 $\Downarrow$   
 abelian  
 or putia sa nu  
 fie abelian

$$\mathbb{F} = \{ \pm 1, \pm i, \pm j, \pm k \}$$

$$(j \cdot k) = k \cdot j, j \cdot k = i, k \cdot j = j$$

$$j \cdot i = -k, k \cdot j = -i, \dots$$

$$i^2 = j^2 = k^2 = -1$$

(unitatile corpului quaternionilor)

$\mathbb{F}$  e necomutativ

$$\mathbb{Z}(6) = \{ \pm 1 \}$$

$$\mathbb{F}/\mathbb{Z}(6) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

Dacă  $g \in \mathbb{F} \setminus \mathbb{Z}(6)$ . Considerăm centralizatorul

dintră  $g$ :  $C(g) = \{ x \in \mathbb{F} \mid xg = gx \} \leq \mathbb{F}$

Dacă  $|\mathbb{F} : C(g)| = 1 \Rightarrow g \in \mathbb{Z}(6) \Rightarrow \emptyset$

•  $|\mathbb{F} : C(g)| = 2$ , de exemplu în grupul quaternionilor  
 $C(i) = \{ \pm 1, \pm i \}$

Concluzie:  $g \in \mathbb{F} \setminus \mathbb{Z}(6) \Rightarrow |\mathbb{F} : C(g)| \geq 2$

Deci

Dacă  $\sigma$  nu este abelian,  $(X, Y) \in \mathcal{G} \times \mathcal{G}$

Cea probabilitate  $\leq \frac{1}{4}$  și comună cu toate elementele

Cea probabilitate  $\geq \frac{3}{4}$ , și comună cu  $\leq \frac{1}{2}$  elemente

Deci  $P(XY=YX) \leq \frac{1}{4} \cdot 1 + \frac{3}{4} \cdot \frac{1}{2} = \frac{5}{8}$

$\left\{ \begin{array}{l} 5/8 \text{ re} \\ \text{atrage} \\ \text{partea grupă} \\ \text{unităților} \\ \text{cavalierești?} \end{array} \right.$

Cercul complex  $C = \{(z_1, z_2) \in \mathbb{C}^2 / |z_1|^2 + |z_2|^2 = 1\}$   
(dim. complexă 2, dim. reală 2)

Algebra quaternională  $Q = \{(z_1, z_2) \in \mathbb{C}^2 / |z_1|^2 + |z_2|^2 = 1\}$   
(dim. reală 3, nu are dim. complexă)

$$\boxed{\begin{aligned} C: & (x_1 + i \cdot y_1)^2 + (x_2 + i \cdot y_2)^2 = 1 \\ \Leftrightarrow & \begin{cases} 1 + y_1^2 + y_2^2 = x_1^2 + x_2^2 \\ x_1 y_1 + x_2 y_2 = 0 \end{cases} \end{aligned}}$$

Cercul complex

$$\boxed{Q: x_1^2 + x_2^2 + y_1^2 + y_2^2 = 1}$$

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

$$(i, \sqrt{2}) \in C \setminus Q$$

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

$$y_1 = 1, y_2 = 0$$

$$\begin{aligned} Q \cap C &= ? \\ x_1^2 + y_1^2 + x_2^2 + y_2^2 &= 1 \quad (1) \\ x_1 y_1 + x_2 y_2 &= 0 \quad (2) \end{aligned}$$

$$\begin{aligned} (1) &\Rightarrow y_1^2 + y_2^2 = 0 \\ &\Rightarrow y_1 = y_2 = 0 \end{aligned}$$

de la prima ec.

de la C

$$x_1^2 + x_2^2 = 1$$

$\boxed{\begin{array}{l} \text{STSAL 2,} \\ \text{f. 10} \end{array}}$

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

$\Rightarrow Q \cap C =$  cerc real de diametru 1

Special Topics in Security and Applied Logic 2 - Curs 7 - 06.04.2023

Un sistem format din  $n$  qubiti.  $\dim = 2^m$

$$H_1 \otimes H_1 \otimes \dots \otimes H_1, \quad H_n = (C, \sum_{i=1}^2 x_i T_i)$$

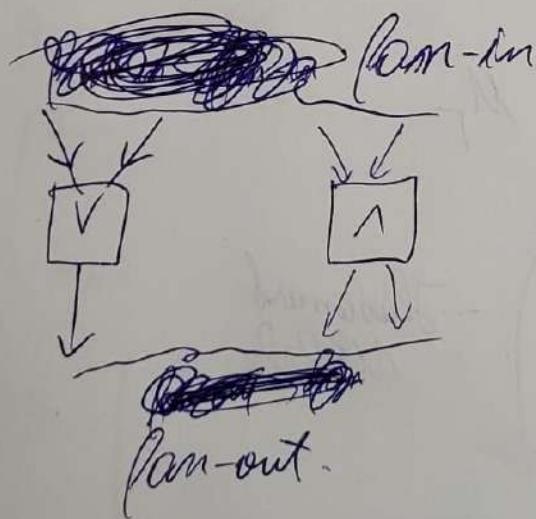
Bara  $\{ |x_1\rangle |x_2\rangle \dots |x_m\rangle \mid x_i \in \{0, 1\} \}$

$2^n$ -elemente; "register cuantic de lungime  $m$ "

Starea registerului:  $C_0 |0\rangle + C_1 |1\rangle + \dots + C_{2^m-1} |2^m-1\rangle$

$$\text{cu conditie } |C_0|^2 + |C_1|^2 + \dots + |C_{2^m-1}|^2 = 1$$

Acasta superpozitie contine  $2^m-1$  numere complexe



Porta cuantica unară:  $U: H_2 \rightarrow H_2$

$$|0\rangle \rightarrow a|0\rangle + b|1\rangle$$

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

a-i. Matricea extinsă este

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \text{ unde } U = (AF) = A^{-1} \overline{F} A = \boxed{7,1}$$

① Negativ

Exemplu: Matricea negativă:

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

$$\begin{matrix} |0\rangle \rightarrow |1\rangle \\ |1\rangle \rightarrow |0\rangle \end{matrix}$$

$M_{cn}$

② "Probabilitatea patrata a negativi":

$$\sqrt{M_F} = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix} \quad "VNU"$$

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

$$\sqrt{M_F} \cdot \sqrt{M_F}^* = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 \Rightarrow \text{Matricea e unitară}$$

$U_{cn}$

$U_{cn}^*$

$U_{cn}$

Produs

File A

B

A =  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

A  $\otimes$  B

Tensore

Periș cuantică binară:  $U: H_4 \rightarrow H_4$

~~$|00\rangle^T = (1, 0, 0, 0)$~~ ;  $|01\rangle^T = (0, 1, 0, 0)$ ;

$|10\rangle^T = (0, 0, 1, 0); |11\rangle^T = (0, 0, 0, 1);$

SALSAL, E  
7.2

File M<sub>1</sub>:

M<sub>2</sub>:

① Negativa condizionale / controllata:

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

$$M_{cnot} \cdot |X_0 X_1\rangle = |X_0, X_0 \oplus X_1\rangle \quad \xrightarrow{\text{Xor}}$$

$$M_{cnot}^* = M_{cnot}$$

$$M_{cnot} \cdot M_{cnot} = id \Rightarrow M_{cnot} \text{ e unitaria}$$

Produs Kronecker / tensorial entre matrice

Ale A - matrice  $n \times n$   
B - matrice  $t \times u$

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{r1} & \dots & a_{rn} \end{pmatrix}$$

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ \vdots & & & \vdots \\ a_{r1}B & a_{r2}B & \dots & a_{rn}B \end{pmatrix}$$

↑  
bloc matrice

Ale  $M_1: H_m \rightarrow H_m$ , atunci  $M_1 \otimes M_2: H_m \otimes H_m \rightarrow H_m \otimes H_m$

$M_2: H_m \rightarrow H_m$  Acum produs tensorial  
nu produce entanglement

STSAL 2.C  
7.3

Exemplu:

$$\text{Iar } M_1 = M_2 = W_2 \text{ (Hadamard Walsh)} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

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

(Obs.:

imentul baselor lui  $H_4$

$$W_4 |X_0 X_1\rangle = \frac{1}{2} (|0\rangle + (-1)^{X_0} |1\rangle) \otimes (|0\rangle + (-1)^{X_1} |1\rangle) =$$

$$= \frac{1}{2} (|00\rangle + (-1)^{X_0} |01\rangle + (-1)^{X_1} |10\rangle + (-1)^{X_0+X_1} |11\rangle)$$

Dacă e decompozabilă!  $W_4$  nu produce entanglement.

(Obs.:

$M_{\text{cnot}}$  nu este produs tensorial ale matrice

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

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

$S$  - decompozabilă.

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

(Einstein, ...)

care e indecompozabilă.  $\Rightarrow$

$\Rightarrow M_{\text{cnot}}$  nu e decompozabilă ca produs tensorial

Teoreme

de von Neumann

$H_m$

$U: H_m \otimes$

$+ k > e$

①: Da cuantum

Dem.:

ipoteze

$$U \left( \frac{1}{\sqrt{2}} \right)$$

$$= \frac{1}{\sqrt{2}}$$

$$\textcircled{2} \quad \frac{1}{\sqrt{2}}$$

$$\Rightarrow \textcircled{6}$$

## Teorema de medonare (Wooters și Zurek)

Este un sistem cu baza  $|a_1\rangle, \dots, |a_n\rangle$   
 $H_m$ ,  ~~$\otimes H_m$~~   $|a_1\rangle$  blank.

$U: H_m \otimes H_m \rightarrow H_m \otimes H_m$ .

$\forall |x\rangle \in H_m$ ,  $U(|x\rangle |a_1\rangle) = |x\rangle |x\rangle$   
"moștra cuantică de copiat"

①: Dacă  $n > 1$ , atunci nu există moștră cuantică de copiat.

Dem.:  $n > 1 \Rightarrow$  există cel puțin 2 stări pure  $|a_1\rangle, |a_2\rangle$  <sub>în ortogonal</sub>

$$\text{ipoteză} \Rightarrow U(|a_1\rangle |a_1\rangle) = |a_1\rangle |a_1\rangle$$

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

$$U\left(\underbrace{\frac{1}{\sqrt{2}}(|a_1\rangle + |a_2\rangle)}_{X}\right) |a_1\rangle \stackrel{\text{②}}{=} U\left(\frac{1}{\sqrt{2}}(|a_1\rangle |a_2\rangle + |a_2\rangle |a_1\rangle)\right) =$$

$$= \frac{1}{\sqrt{2}}|a_1\rangle |a_1\rangle + \frac{1}{\sqrt{2}}|a_2\rangle |a_2\rangle \quad \leftarrow \text{entangled.}$$

$$\text{② } \frac{1}{\sqrt{2}}(|a_1\rangle + |a_2\rangle) \cdot \frac{1}{\sqrt{2}}(|a_1\rangle + |a_2\rangle) \quad \leftarrow \text{decompozabil}$$

$\Rightarrow X$

$\mathbb{F}_2 = \mathbb{F}_2$

Item coe  $2V, 1, \Gamma$  formeză o familie completă de funcții:

$f: \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m$  se poate scrie ca un tuplu de expresii booleane.

Circuit boolean: Graf aciclic orientat

$X_i$  - variabile de intrare

$T_j$  - variabile de ieșire

$V, V$  - fan-in = 2  
fan-out  $\geq 1$

$\Gamma$  - fan-in = 1  
fan-out  $\geq 1$

O operatie/poarta reversibilă este o

$f: \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m$   
bijectivă

Exemplu 1: Poarta Toffoli

$$T(X_1, X_2, X_3) = (X_1, X_2, \textcircled{X}_3, X_1X_2 + X_3)$$

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

Ex 2: Negatoră controlată

$$N: \mathbb{F}_2^2 \rightarrow \mathbb{F}_2^2, N(X_1, X_2) = (X_1, X_1 + X_2)$$

\* Dacă  
 $\Rightarrow \exists$

$\wedge X_1 \dots$

Lemă: ?

Dem.:

• Observație

$\Rightarrow$  putem

$\wedge V \vee X$

•  $N(X)$

(T)  $\Rightarrow$  000

Dom: T(1,1)  
T(1,X)

Circuit reversibil: permutare a lui  $F_2^n$  compusa din operări reversibile.

\* Dacă  $C(X_1, \dots, X_n)$  este o funcție booleană oricare  $\Rightarrow \exists f: F_2^{n+m} \rightarrow F_2^{n+m}$  și  $c_1, \dots, c_m \in F_2$  constante a.t.

$$\forall X_1, \dots, X_n \in F_2, f(X_1, \dots, X_n, c_1, \dots, c_m) = (C(X_1, \dots, X_n), d_1, \dots, d_m)$$

Lemă:  $\{T, N, T\}$  - multime universală, necesită doar constantă 0.

Dem.: • negație și reversibilitate poată fi folosite direct

- Observăm că  $T(X_1, X_2, 0) = (X_1, X_2, X_1 X_2) \Rightarrow$  putem calcula conjunctia.
- $X_1 \vee X_2 = \cancel{\text{X}_1 \oplus \text{X}_2} \Rightarrow (T(X_1, 1 \wedge X_2)) \Rightarrow$  putem calcula disjunctia.
- $N(X_0, 0) = (X_0, X_0) \Rightarrow$  putem simula portă cu fan-out  $> 1$

(T) Poarta Toffoli este poarta reversibilă universală.

Din:  $T(1, 1, X) = (1, 1, 1 \cdot X) \Rightarrow$  se poate obține 1

$T(1, X, 1) = (1, X, X + 1) \Rightarrow$  se poate obține N

□

$\vec{x} \in F_2^m$  identic,  $|\vec{x}\rangle = l_i = (0, 0, \dots, \overset{i}{1}, 0, \dots, 0)^T$

unde  $\vec{x}$  reprezintarea binara a lui  $i+1$

$$T_{(8 \times 8)} = \begin{pmatrix} I_2 & 0 & 0 & 0 \\ 0 & I_2 & 0 & 0 \\ 0 & 0 & I_2 & 0 \\ 0 & 0 & 0 & M_T \end{pmatrix}$$

Modificari stricte  $x_0 x_1 x_2$  numai in carurile

$$\begin{array}{l} 110 \rightsquigarrow 111 \text{ adica } l_4 \rightsquigarrow l_3 \\ 111 \rightsquigarrow 110 \text{ adica } l_4 \rightsquigarrow l_2 \end{array}$$

Esercizi:

Fie 5-grup finit. P - probabilitatea evenimentului

$$C = \{(x, t) \in 5 \times 5 \mid xy = yx\}$$

(1) Daca  $P = P(C) > \frac{5}{8} \Rightarrow 5$  este abelian

Dem: Fie central grupului  $Z(5) =$

$$= \{x \in 5 \mid \forall y \quad xy = yx\} \trianglelefteq 5$$

Daca  $|5 : Z(5)| = 1 \Rightarrow 5 = Z(5)$  (subgrup normal)

$\bullet |5 : Z(5)| = 2 \Rightarrow \exists u, v \in 5 \quad u \notin Z(5) \Rightarrow$

(indice 2)  $\Rightarrow \forall y \in Z(5) \quad u^y \notin Z(5) \Rightarrow$

$$X = uY \quad \text{stare} \quad \boxed{7-8}$$

$15 : Z(5)$

$\Rightarrow 6$

$15 : Z(5)$

$5 = 3 \pm 1$

$c_j = k$

$j^i = -k$

$i^2 = j^2 =$

Cantitate

$t$  e recom

$Z(5) = \{f$

$\overline{f} / Z(f) \cong$

Daca  $g \in$

leu g : C(g)

Daca  $|5 : C(g)| =$

$|5 : C(g)| = 2$

Concluzie:  $g \in$

$\Rightarrow \mathbb{F} = \langle \mathbb{Z}(6), u \rangle \Rightarrow \mathbb{F}$ -abelian.

•  $|\mathbb{F} : \mathbb{Z}(6)| = 3 \Rightarrow \mathbb{F} = \mathbb{Z}(6) \cup a \cdot \mathbb{Z}(6) \cup a^2 \cdot \mathbb{Z}(6)$

$\Rightarrow \mathbb{F} = \langle \mathbb{Z}(6), a \rangle \Rightarrow \mathbb{F}$ -abelian.

•  $|\mathbb{F} : \mathbb{Z}(6)| = 4 \Rightarrow \text{num } \mathbb{F}/\mathbb{Z}(6) = \mathbb{Z}_4$  num  $\mathbb{F}/\mathbb{Z}(6) = \mathbb{Z}_2 \times \mathbb{Z}_2$   
abellian or putia nu  
este abelian

$$\mathbb{F} = \{ \pm 1, \pm i, \pm j, \pm k \}$$

$$ij = k, jk = i, ki = j$$

$$ji = -k, kj = -i, ...$$

$$i^2 = j^2 = k^2 = -1$$

(unitatile corpului cuaternionilor)

$\mathbb{F}$  e necomutativ

$$\mathbb{Z}(6) = \{ \pm 1 \}$$

$$\mathbb{F}/\mathbb{Z}(6) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

Dacă  $g \in \mathbb{F} \setminus \mathbb{Z}(6)$ . Considerăm centralizatorul

$$\text{leu } g : C(g) = \{ x \in \mathbb{F} \mid xg = gx \} \trianglelefteq \mathbb{F}$$

$$\text{Dacă } |\mathbb{F} : C(g)| = 1 \Rightarrow g \in \mathbb{Z}(6) \Rightarrow \emptyset$$

•  $|\mathbb{F} : C(g)| = 2$ , de exemplu în grupul cuaternionilor  
 $C(i) = \{ \pm 1, \pm i \}$

Bunăstătare:  $g \in \mathbb{F} \setminus \mathbb{Z}(6) \Rightarrow |\mathbb{F} : C(g)| \geq 2$

STRATEGIE  
7.9

Deci  
Dacă 5 nu e abalon,  $(x_1, y) \in \mathbb{S} \times \mathbb{S}$

Cu probabilitate  $\leq \frac{1}{4}$  x comunită cu toate elementele

Cu probabilitate  $\geq \frac{3}{4}$ , x comunită cu  $\leq \frac{1}{2}$  elemente

Deci  $P(XY=YX) \leq \frac{1}{4} \cdot 1 + \frac{3}{4} \cdot \frac{1}{2} = \frac{5}{8}$   $\left\{ \begin{array}{l} 5/8 \text{ re} \\ \text{atâtice} \\ \text{pentru grupuri} \\ \text{unităților} \\ \text{căutării mănușelor?} \end{array} \right.$

Cercul complet  $C = \{(z_1, z_2) \in \mathbb{C}^2 / |z_1|^2 + |z_2|^2 = 1\}$   
(dim. complexă 1, dim. reală 2)

Spația qubitelor  $Q = \{(z_1, z_2) \in \mathbb{C}^2 / |z_1|^2 + |z_2|^2 = 1\}$   
(dim. reală 3, nu are dim. complexă)

$$\boxed{\begin{aligned} C: & (x_1 + i \cdot y_1)^2 + (x_2 + i \cdot y_2)^2 = 1 \\ \Leftrightarrow & \begin{cases} x_1^2 + y_1^2 + y_2^2 = x_1^2 + x_2^2 \\ x_1 y_1 + x_2 y_2 = 0 \end{cases} \end{aligned}}$$

Cercul complet.

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

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

$$(i, 1/\sqrt{2}) \in C \setminus Q$$

$$x_1 = 0, x_2 = 1/\sqrt{2}$$

$$y_1 = 1, y_2 = 0$$

$$\begin{cases} Q \cap C = ? \\ x_1^2 + y_1^2 + y_2^2 + y_1^2 + y_2^2 = 1 \quad (1) \\ x_1 y_1 + x_2 y_2 = 0 \quad (2) \end{cases}$$

$$\Rightarrow \boxed{y_1^2 + y_2^2 = 0}$$

$$\Rightarrow \boxed{y_1 = y_2 = 0}$$

din prima ec.

din loc. C

$$x_1^2 + x_2^2 = 1$$

$$\Rightarrow (X_1, X_2, Y_1, Y_2) = (\sin \theta, \cos \theta, 0, 0)$$

$\Rightarrow Q \cap C$  = cerc real de diametru 1