Curs 6 STLS II

Quantum Computing

Decizie: $\langle^{n}_{Prim(n)}$ // 2003 - AKS lungime timp polinomial în $l(n)$

PRIME ∈ coNP ⇔ COMPOSITE ∈ NP

PRIME ∈ P (timp polinomial)

RSA: $d = e^{-1} \bmod (p-1)(q-1)$, unde $N = \underbrace{pq}_{\text{info publică}}$ $\underbrace{\quad}_{\text{info secretă}}$

Schor: În Quantum Computing, factorizarea este (National Institute of Standards in Technology) fezabilă cu complexitate polinomială dar și DLP (logaritmul discret)

NIST: 80' - DES (Horst Feistel + co.) criptare bloc 64

90' - 2000 - AES (Rijmen, Dakhnal) criptare bloc 128

2020 "post-quantum security"

- non-determinism cuantic (intrinsec universului)

electron e^- $\Psi: \mathbb{R}^3 \to \mathbb{C}$ funcția de undă $\quad prob = \int_A |\Psi(x)|^2 dx$

Sistem probabilist = mulțime finită de stări $x_1, \dots, x_n$

Stabil: p_i = probabilitatea ca sistemul să se afle în starea x_i.

Distribuția de probabilitate: $p_1[x_1] + p_2[x_2] + \dots + p_n[x_n]$; momentul T0

$p_i \geq 0$, $p_1 + p_2 + \dots + p_n = 1$

monedă (head, tail) $\frac{1}{2}h + \frac{1}{2}t$.

Markov. Fie p_{ij} probabilitatea ca sistemul să treacă din starea x_i în starea x_j.

$$\begin{cases} [x_i] \longrightarrow p_{i1}[x_1] + p_{i2}[x_2] + \dots + p_{in}[x_n] \\ p_{ij} \geq 0, \quad p_{i1} + p_{i2} + \dots + p_{in} = 1. \end{cases}$$

T_1 $p_1 \left(p_{11}[x_1] + p_{12}[x_2] + \dots + p_{1n}[x_n] \right) +$
$p_2 \left(p_{21}[x_1] + p_{22}[x_2] + \dots + p_{2n}[x_n] \right) + \dots$

$$\begin{pmatrix} p_1' \\ p_2' \\ \vdots \\ p_n' \end{pmatrix} = \underbrace{\begin{pmatrix} p_{11} & p_{12} & \dots & p_{1n} \\ p_{21} & p_{22} & \dots & p_{2n} \\ & & \dots & \\ p_{n1} & p_{n2} & \dots & p_{nn} \end{pmatrix}}_{=A} \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix}$$

suma pe fiecare linie este egală cu 1

matrice Markov, matrice stocastică

$\vec{p}' = A\vec{p}$

T_0 T_1
$\vec{p}, A\vec{p}, A^2\vec{p}, \dots, A^n\vec{p}$ — lanț Markov

Sistem cuantic (extinde not. probabilist)

Nr. finit de stări $x_1, x_2, \dots, x_n$; formal generează un spațiu Hilbert $H_n = \mathbb{C}^n$

bază ortogonală $\{|x_1\rangle, |x_2\rangle, \dots, |x_n\rangle\}$

Notație: $|a\rangle$ = ket ; $\langle a|$ = bra

$\langle a|b\rangle$ = braket, produs Hermitian

$\overline{x+iy} = x - iy$

$(a_1, \dots, a_n) \begin{pmatrix} \overline{b_1} \\ \overline{b_2} \\ \vdots \\ \overline{b_n} \end{pmatrix} |b\rangle$

$\langle a|$

• stare a sistemului cuantic: „superpoziție a stărilor de bază" $\alpha_i \in \mathbb{C}$

$\alpha_1 |x_1\rangle + \alpha_2 |x_2\rangle + \dots + \alpha_n |x_n\rangle$ unitar i.e:

$|\alpha_1|^2 + |\alpha_2|^2 + \dots + |\alpha_n|^2 = 1$, unde $x, y \in \mathbb{R}$

$|x + iy|^2 = x^2 + y^2$

• probabilitatea stării $|x_i\rangle$ este $|\alpha_i|^2$

• $\psi(x_i) = \alpha_i$ funcție de undă $p = |\psi(x_i)|^2$

• Dacă $|x\rangle = e^{i\theta} |y\rangle$, stările $|x\rangle$ și $|y\rangle$ sunt echivalente

• bit: sistem macroscopic cu două stări (ex: semafor)

• qubit: sistem cuantic cu două stări

stare a unui qubit: $\alpha_0 |0\rangle + \alpha_1 |1\rangle$ $\alpha_{0,1} \in \mathbb{C}$

a.î. $|\alpha_0|^2 + |\alpha_1|^2 = 1$.

$$\begin{pmatrix} \alpha_1' \\ \alpha_2' \\ \vdots \\ \alpha_n' \end{pmatrix} = \underbrace{\begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1m} \\ & & & \\ \alpha_{m1} & & & \alpha_{mm} \end{pmatrix}}_{A} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_m \end{pmatrix}$$

adjunct: $A^* = \overline{A}^T$ — conjugat transpus

Atunci $A^* = A^{-1}$ operator unitar

Operatorii unitari sunt inversabili → Procesele de calcul cuantic sunt reversibile

Ex monedă cuantică

$|h\rangle \to \frac{1}{\sqrt{2}} |h\rangle + \frac{1}{\sqrt{2}} |t\rangle$

$|t\rangle \to \frac{1}{\sqrt{2}} |h\rangle - \frac{1}{\sqrt{2}} |t\rangle$

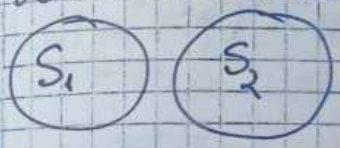
Obs. $|\alpha_{ij}|^2 = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$

$A = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$ $\quad \overline{A}^T = A = A^{-1} \quad A \cdot A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ identitatea

Hadamard Walsh

A operator unitar

Ex Două sisteme cuantice



H_n: $|x_1\rangle, \dots, |x_n\rangle$ stări cuantice fundamentale
$|y_1\rangle, \dots, |y_m\rangle$ H_m

$(|x_i\rangle, |y_j\rangle) \rightsquigarrow |x_i y_j\rangle$

$H_n \otimes H_m$ = spațiu vectorial de dimensiune $m \cdot n$.

produs tensorial

$|x_i\rangle \otimes |y_j\rangle = |x_i y_j\rangle$

$\sum_{\substack{i=\overline{1,n} \\ j=\overline{1,m}}} \alpha_{ij} |x_i y_j\rangle = \left(\sum_{i=1}^{n} \alpha_i |x_i\rangle\right)\left(\sum_{j=1}^{m} \beta_j |y_j\rangle\right)$ $\Leftrightarrow$ stare decomporabilă (*)

sisteme independente $\Leftrightarrow$ sistemul reunione este produsul superpozițiilor celor două sisteme considerate separat

Exemplu: doi Qubiți Q_1, Q_2

$Q_1 \cup Q_2 : \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$ entanglement

(*) negație: stare indecomporabilă (entangled)

stare decomporabilă (reuniunea de doi qubiți)

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

Exemplu: Einstein, Podolski, Rosen $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ stare dorită

EPR state $\rightarrow$ entangled

Pp absurd $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = (\alpha|0\rangle + \beta|1\rangle) \cdot (\gamma|0\rangle + \delta|1\rangle) =$

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

$\alpha, \beta, \gamma, \delta \in \mathbb{C}$ $\quad |\alpha|^2 + |\beta|^2 = |\gamma|^2 + |\delta|^2 = 1$

$$\begin{cases} \alpha\gamma = \frac{1}{\sqrt{2}} \\ \alpha\delta = 0 \\ \beta\gamma = 0 \\ \beta\delta = \frac{1}{\sqrt{2}} \end{cases}$$

$\alpha\delta = 0, \beta\gamma = 0 \Rightarrow (\alpha = 0 \vee \delta = 0) \wedge (\beta = 0 \vee \gamma = 0)$ ✗ nu este satisfiabilă în $\mathbb{C}$.

Completare teoria codurilor

MacWilliams (Exam): $A^{\perp}(z) = q^{-k}(1+(q-1)z)^n A\left(\frac{1-z}{1+(q-1)z}\right)$

$C = \{(\underbrace{0,0,\dots,0}_{n}), (\underbrace{1,1,\dots,1}_{n})\} \subseteq \mathbb{F}_2^n$

$C^{\perp} = \{\vec{v} \in \mathbb{F}_2^n \mid wt(\vec{v}) \in 2\mathbb{N}\}$

$A(z) = 1 + z^n$ $\quad A^{\perp}(z) = \frac{1}{2}(1+z)^n\left(1+\left(\frac{1-z}{1+z}\right)^n\right) =$

$= \frac{1}{2}\left[(1+z)^n + (1-z)^n\right] =$

$= \frac{1}{2}\left[\sum_{k=0}^{n}\binom{n}{k}z^k + \sum_{k=0}^{n}\binom{n}{k}(-1)^k z^k\right] =$

$= \frac{1}{2}\sum_{i\geq 0} 2\binom{n}{2i}z^{2i} = \sum_{i\geq 0}\binom{n}{2i}z^{2i}$

$C = \{(0,0,0,0), (1,1,1,1), (2,2,2,2)\} \subseteq \mathbb{F}_3^4$

$A(z) = 1 + 2z^4$ $\quad A^{\perp}(z) = \frac{1}{3}(1+2z)^4\left[1+2\left(\frac{1-z}{1+2z}\right)^4\right] =$

$= \frac{1}{3}\left[(1+2z)^4 + 2(1-z)^4\right] =$

$$= \frac{1}{3}\left[1+8z+24z^2+32z^3+16z^4+2-8z+12z^2-8z^3+2z^4\right]$$

$$= \frac{1}{3}\left(3+36z^2+24z^3+18z^4\right) = 1+12z^2+8z^3+6z^4$$

Q.C.

Ex moneda corectă $M = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$. Calc. $M^2 = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} = M$

Deci $M^n = M$, $\forall n$

Nu există efect cumulativ în acest caz (cel mai simplu fenomen Markov)

moneda incorectă $M = \begin{pmatrix} 1-\varepsilon & \varepsilon \\ 1-\varepsilon & \varepsilon \end{pmatrix}$. Calc. $M^2 = \begin{pmatrix} (1-\varepsilon)^2+\varepsilon(1-\varepsilon) & (1-\varepsilon)\varepsilon+\varepsilon^2 \\ (1-\varepsilon)^2+\varepsilon(1-\varepsilon) & (1-\varepsilon)\varepsilon+\varepsilon^2 \end{pmatrix} =$

$\varepsilon \in (0, \frac{1}{2})$

$$= \begin{pmatrix} -\varepsilon+1 & \varepsilon \\ -\varepsilon+1 & \varepsilon \end{pmatrix} = M$$

Deci $M^n = M$, $\forall n$

Deci mici monedă incorectă nu are efect cumulativ.

Ex $M = \begin{pmatrix} 1-\varepsilon & \varepsilon \\ \varepsilon & 1-\varepsilon \end{pmatrix}$ $\varepsilon \neq \frac{1}{2}$ $M^2 \neq M$

$\lim_{n\to\infty} M^n = ?$

Ec. caracteristică: $\det(iX - M)$

$$(X-1+\varepsilon)^2 - \varepsilon^2 = 0$$

$$(X-1+2\varepsilon)(X-1) = 0 \Rightarrow \begin{cases} X_1 = 1 \\ X_2 = 1-2\varepsilon \end{cases}$$ valori proprii

$\begin{pmatrix} 1-\varepsilon & \varepsilon \\ \varepsilon & 1-\varepsilon \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$ $\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ vector propriu

$\begin{pmatrix} 1-\varepsilon & \varepsilon \\ \varepsilon & 1-\varepsilon \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1-2\varepsilon \\ \text{scalar} \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}$ $\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ vector propriu

$\begin{pmatrix} 1 \\ 1 \end{pmatrix} \perp \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ ortogonali

$W_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ $W_2^{-1} = W_2$

$M = W_2 \cdot D \cdot W_2$, unde $D = \begin{pmatrix} 1 & 0 \\ 0 & 1-2\varepsilon \end{pmatrix}$ matricea diagonală a valorilor proprii

$M^n = W_2 D^n W_2$ $n \to \infty$: $D^n \to \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

$$M^n \to \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}$$

Deci $M^n \xrightarrow[n\to\infty]{} \begin{pmatrix}1/2 & 1/2\\ 1/2 & 1/2\end{pmatrix}$.

Curs 6 RE

Binare statice și binare dinamice

stack overflow (seg fault) — 80

(+ only data)