Quantum Computing

Mihai Prunescu*

Abstract

Pasaje alese, simplificate si traduse din cartea *Quantum Computing* de Mika Hirvensalo.

*University of Bucharest, Faculty of Mathematics and Informatics; and Simion Stoilow Institute of Mathematics of the Romanian Academy, Research unit 5, P. O. Box 1-764, RO-014700 Bucharest, Romania.
mihai.prunescu@imar.ro, mihai.prunescu@gmail.com

Contents

Part I
Curs

1 Sistem probabilist

Un sistem probabilist are un numar finit de stari $x_1, \ldots, x_n$. Se cunoaste probabilitatea p_i ca sistemul sa se afle in starea i. Distributia de probabilitate se noteaza:

$$p_1[x_1] + p_2[x_2] + \cdots + p_n[x_n],$$

unde $p_i \geq 0$ si $p_1 + p_2 + \cdots + p_n = 1$.

Exemplu: O moneda are cap **head** si ban **tail**. Ea se reprezinta ca distributia de probabilitate:

$$\frac{1}{2}h + \frac{1}{2}t.$$

□

Fie p_{ij} probabilitatea ca sistemul sa treaca din starea x_i in starea x_j. Cu alte cuvinte, are loc urmatoarea inlocuire de distributii de probabilitate:

$$[x_i] \to p_{i1}[x_1] + p_{i2}[x_2] + \cdots + p_{in}[x_n],$$

unde $p_{i1} + p_{i2} + \cdots + p_{in} = 1$. Rezulta ca distributia de probabilitate

$$p_1[x_1] + p_2[x_2] + \cdots + p_n[x_n],$$

se transforma in distributia de probabilitate

$$p_1(p_{11}[x_1] + p_{21}[x_2] + \cdots + p_{n1}[x_n]) + \cdots + p_n(p_{1n}[x_1] + p_{2n}[x_2] + \cdots + p_{nn}[x_n]) =$$

$$= p'_1[x_1] + p'_2[x_2] + \cdots + p'_n[x_n],$$

adica

$$\begin{pmatrix} p'_1 \\ p'_2 \\ \vdots \\ p'_n \end{pmatrix} = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n1} & p_{n2} & \cdots & p_{nn} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix}.$$

Aceasta este o **matrice Markov**, si evolutia distributiei de probabilitate se numeste **lant Markov** sau **proces Markov**.

2 Sistem cuantic

Un sistem cuantic are starile fundamentale $x_1, x_2, \ldots, x_n$. Spatiul de stari al unui sistem cuantic este spatiul vectorial H_n de dimensiune n peste corpul $\mathbb{C}$. Acest spatiu are o baza ortonormala $\{|x_1\rangle, |x_2\rangle, \ldots, |x_n\rangle\}$. Aceasta este notatia **ket** si vine din descompunerea cuvantului **braket** care se refera la produsul hermitian $\langle x, y\rangle$. Vom reveni mai tarziu asupra acestei notatii. Starile x_i se numesc stari de baza.

O **stare** a sistemului cuantic este un vector unitar:

$$\alpha_1|x_1\rangle + \alpha_2|x_2\rangle + \cdots + \alpha_n|x_n\rangle,$$

unde $\alpha_i \in \mathbb{C}$ iar **unitar** inseamna $|\alpha_1|^2 + |\alpha_2|^2 + \cdots + |\alpha_n|^2 = 1$. Probabilitatea ca sistemul sa se afle in starea x_i este $|\alpha_i|^2$. Starea este o **superpozitie** de stari de baza. Aplicatia $\psi(x_i) = \alpha_i$ se numeste **functie de unda**.

Daca $|x\rangle = e^{i\theta}|y\rangle$ spunem ca starile $|x\rangle$ si $|y\rangle$ sunt **echivalente**.

Exemplu: Un **qubit** este un sistem cuantic format din doua stari. Se alege baza ortonormala $\{|0\rangle, |1\rangle\}$ si o stare generala a sistemului este $\alpha_0|0\rangle + \alpha_1|1\rangle$ cu $|\alpha_0|^2 + |\alpha_1|^2 = 1$. □

Evolutia unui sistem cuantic este data de o relatie:

$$\begin{pmatrix} \alpha_1' \\ \alpha_2' \\ \vdots \\ \alpha_n' \end{pmatrix} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}.$$

De data aceasta conditia pe care trebuie sa o indeplineasca matricea A este de a fi o matrice **unitara**, adica:

$$A^* :=^T \overline{A} = A^{-1}.$$

Matricea $A^* =^T \overline{A}$ se numeste si **adjuncta** lui A. Reamintim ca ${}^T A$ este operatia de transpozitie iar $\overline{A}$ este conjugarea complexa a elementelor matricii.

Observatie: Operatiile unitare sunt in particular **inversabile**. De aceea dispozitivele cuantice de calcul sunt in general **reversibile**. Asupra acestui aspect se va reveni in contextul circuitelor cuantice.

Exemplu: Dam cu banul cuantic (o posibilitate...)

$$\begin{aligned} |h\rangle &\rightarrow \frac{1}{\sqrt{2}}|h\rangle + \frac{1}{\sqrt{2}}|t\rangle \\ |t\rangle &\rightarrow \frac{1}{\sqrt{2}}|h\rangle - \frac{1}{\sqrt{2}}|t\rangle \end{aligned}$$

Aplicatia este unitara. Pornind din starea $|h\rangle$, cele doua stari apar cu probabilitate de $1/2$ fiecare. Dar la a doua aruncare, ne intoarcem in starea $|h\rangle$. □

Fie doua sisteme cuantice cu stari de baza $|x_1\rangle$, ..., $|x_n\rangle$ respectiv $|y_1\rangle$, ..., $|y_m\rangle$. Reuniunea celor doua sisteme are ca stari de baza perechi $(|x_i\rangle, |y_j\rangle) := |x_i y_j\rangle$, iar starea reuniunii celor doua sisteme are forma:

$$\sum_{i=1}^{n}\sum_{j=1}^{m} \alpha_{ij}|x_i y_j\rangle.$$

Daca doua spatii vectoriale H_n si H_m au bazele $|x_1\rangle$, ..., $|x_n\rangle$ respectiv $|y_1\rangle$, ..., $|y_m\rangle$, spatiul vectorial $H_n \otimes H_m$ are baza formata din cei nm vectori $|x_i y_j\rangle$, care nu sunt altceva decat perechi $|x_i\rangle \otimes |y_j\rangle = |x_i y_j\rangle$. Produsul tensorial este bilinear:

$$(\sum_{i=1}^{n} \alpha_i|x_i\rangle) \otimes (\sum_{j=1}^{m} \beta_j|y_j\rangle) = \sum_{i=1}^{n}\sum_{j=1}^{m} \alpha_i\beta_j|x_i y_j\rangle.$$

Daca starea sistemului compus poate fi scrisa ca un produs tensorial de stari, starea este **decompozabila**. Altfel, starea este **indecompozabila** sau **entangled**.

Exemplu: Fie un sistem format din doi qubiti. Starea:

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

este decompozabila. Intr-adevar,

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

□

Exemplu: Fie un sistem format din doi qubiti. Starea:

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

este entangled. Aceasta se numeste **pereche EPR** sau pereche Einstein - Podolski - Rosen. Starile $|00\rangle$ si $|11\rangle$ se observa cu probabilitate de $1/2$ pe cand starile $|01\rangle$ sau $|10\rangle$ se vor observa cu probabilitate 0. Asadar

$$P[S(Q_1) = S(Q_2)] = 1.$$

Particulele pastreaza starea entangled chiar daca sunt la distanta mare una de alta. Asta ofera posibilitati pentru criptografia cuantica si pentru protocoalele cuantice de comunicatie. □

Un sistem format din m qubiti este descris de spatiul vectorial $H_2 \otimes H_2 \otimes \cdots \otimes H_2$. Acest spatiu are baza formata din vectorii $|x_1\rangle|x_2\rangle \ldots |x_m\rangle$ unde $(x_1, \ldots, x_m) \in \{0,1\}^m$. Spatiul are dimensiune 2^m si se numeste **registru cuantic de lungime m**.

Starea generala a registrului quantic de m qubiti este data de o expresie:

$$c_0|0\rangle + c_1|1\rangle + \cdots + c_{2^m-1}|2^m - 1\rangle,$$

cu conditia $|c_0|^2 + \cdots + |c_{2^m-1}|^2 = 1$. Aceasta descriere necesita $O(2^m)$ numere complexe. Deci ponderea descrierii unei stari creste exponential in ponderea fizica a sistemului. Asa se explica intr-o anumita masura performanta calculatoarelor cuantice.

3 Informatie cuantica

O operatie pe un qubit, numita **poarta cuantica unara**, este o aplicatie unitara $U : H_2 \to H_2$. Ea are forma:

$$\begin{aligned} |0\rangle &\to a|0\rangle + b|1\rangle \\ |1\rangle &\to c|0\rangle + d|1\rangle \end{aligned}$$

unde

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a^* & c^* \\ b^* & d^* \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Aceasta relatie este explicitarea caracterului unitar. Notatia a^* semnifica din nou conjugarea numerelor complexe.

Exemplu: Fie reprezentarea $|0\rangle =^T (1,0)$ si $|1\rangle =^T (0,1)$. Matricea unitara:

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

defineste actiunea $M_\neg|0\rangle = |1\rangle$, $M_\neg|1\rangle = |0\rangle$. Aceasta poarta cuantica se numeste **negatie cuantica**. □

Exemplu: Consideram poarta cuantica data de aplicatia unitara:

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

Observam ca

$$\sqrt{M_\neg}|0\rangle = \frac{1+i}{2}|0\rangle + \frac{1-i}{2}|1\rangle,$$

si cum

$$\left|\frac{1+i}{2}\right|^2 = \left|\frac{1-i}{2}\right|^2 = \frac{1}{2},$$

rezultatele $|0\rangle$ si $|1\rangle$ se vor vedea cu probabilitate egala cu $1/2$. Aceasta operatie se numeste **radacina patrata a negatiei cuantice**. □

Exemplu: Operatia W_2 data de matricea unitara:

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

se numeste **matricea Hadamard-Walsh**. □

O **poarta cuantica binara** este o aplicatie unitara $U : H_4 \to H_4$. Folosim urmatoarea reprezentare: $|00\rangle =^T (1,0,0,0)$, $|01\rangle =^T (0,1,0,0)$, $|10\rangle =^T (0,0,1,0)$, $|11\rangle =^T (0,0,0,1)$.

Exemplu: Matricea unitara:

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

defineste operatie de **negatie cuantica controlata**. Se verifica faptul ca:

$$M_{\text{cnot}}|x_0x_1\rangle = |x_0, x_0 +_2 x_1\rangle.$$

Deci al doilea qubit este negat daca si numai daca primul qubit (qubitul **de control**) este 1. □

Produsul tensorial sau **produsul Kronecker** al unei matrici $r \times s$ notata A cu o matrice $t \times u$ notata B dupa cum urmeaza:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1s} \\ a_{21} & a_{22} & \dots & a_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r1} & a_{r2} & \dots & a_{rs} \end{pmatrix} \quad ; \quad B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1u} \\ b_{21} & b_{22} & \dots & b_{2u} \\ \vdots & \vdots & \ddots & \vdots \\ b_{t1} & b_{t2} & \dots & b_{tu} \end{pmatrix}$$

este matricea $rt \times su$ notata $A \otimes B$ care are urmatoarea reprezentare bloc:

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1s}B \\ a_{21}B & a_{22}B & \dots & a_{2s}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{r1}B & a_{r2}B & \dots & a_{rs}B \end{pmatrix}.$$

Daca $M_1 : H_n \to H_n$ iar $M_2 : H_m \to H_m$ atunci $M_1 \otimes M_2 : H_n \otimes H_m \to H_n \otimes H_m$. Se observa ca $M_1 \otimes M_2$ **nu introduce entanglement** intre H_n si H_m.

Exemplu: Fie $M_1 = M_2 = W_2$, matricea Hadamard-Walsh. Actiunea pe ambii qubiti a matricii Hadamard-Walsh poate fi vazuta ca poarta cuantica binara, definita de matricea:

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

Se observa ca:

$$W_4|x_0x_1\rangle = \frac{1}{2}(|0\rangle + (-1)^{x_0}|1\rangle) \otimes (|0\rangle + (-1)^{x_1}|1\rangle) =$$

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

Cu alte cuvinte se observa ca aceasta stare este decompozabila.

Observatie: Negatia controlata M_{cnot} nu poate fi descompusa ca produs tensorial de matrici.

Intr-adevar consideram starea decompozabila:

$$S = (W_2 \otimes I_2)\ |00\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle).$$

Se observa ca $M_{\text{cnot}}S$ este o stare entangled:

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

Asta nu s-ar putea daca M_{cnot} ar fi decompozabila. □

Nu orice operatie se poate face folosind porti cuantice. Vom prezenta Teorema de Neclonare a lui W. K. Wooters si W. H. Zurek. Fie un sistem cuantic cu starile de baza $|a_1\rangle, \ldots, |a_n\rangle$. Fie H_n spatiul starilor. Consideram ca starea $|a_1\rangle$ are functia de **blanc**.

Definitie: *O functie unitara $U : H_n \otimes H_n \to H_n \otimes H_n$ cu proprietatea ca pentru orice stare $|x\rangle \in H_n$ are loc:*

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

se numeste masina cuantica de copiat.

Teorema de Neclonare: *Daca $n > 1$ nu exista nicio masina cuantica de copiat.*

Demonstratie: Presupunem ca U exista si ca $n > 1$. Deoarece $n > 1$, exista doua stari ortogonale, in particular starile de baza $|a_1\rangle$ si $|a_2\rangle$. Dar $U(|a_1\rangle|a_1\rangle) = |a_1\rangle|a_1\rangle$ si $U(|a_2\rangle|a_1\rangle) = |a_2\rangle|a_2\rangle$. Mai mult:

$$U\Big(\frac{1}{\sqrt{2}}(|a_1\rangle + |a_2\rangle)|a_1\rangle\Big) = \Big(\frac{1}{\sqrt{2}}(|a_1\rangle + |a_2\rangle))(\frac{1}{\sqrt{2}}(|a_1\rangle + |a_2\rangle)\Big) =$$

$$= \frac{1}{2}\Big(|a_1\rangle|a_1\rangle + |a_1\rangle|a_2\rangle + |a_2\rangle|a_1\rangle + |a_2\rangle|a_2\rangle\Big).$$

Pe de alta parte din linearitate:

$$U\Big(\frac{1}{\sqrt{2}}(|a_1\rangle + |a_2\rangle)|a_1\rangle\Big) = \frac{1}{\sqrt{2}}U(|a_1\rangle|a_1\rangle) + \frac{1}{\sqrt{2}}U(|a_2\rangle|a_1\rangle) =$$

$$= \frac{1}{\sqrt{2}}|a_1\rangle|a_1\rangle + \frac{1}{\sqrt{2}}|a_2\rangle|a_2\rangle.$$

Cele doua reprezentari sunt diferite. Contradictie. □

4 Masini Turing cuantice

Pentru a defini o masina Turing cuantica, consideram un **alfabet** finit A, o multime finita de **stari** ale masinii Q, si trei stari speciale $q_0, q_a, q_r \in Q$ numite starea **initiala**, starea **acceptanta** si starea **neganta**. Ultimile doua stari sunt stari **finale**. Pe deasupra se defineste o functie de **amplitudine** a tranzitiilor posibile:

$$\delta : Q \times A \times Q \times A \times \{-1, 0, 1\} \to \mathbb{C}.$$

O **configuratie** a masinii Turing este un tuplu (q, w_1, a, w_2) unde $q \in Q$, $a \in A$ iar w_1, w_2 sunt cuvinte peste A. Spatiul vectorial complex generat de configuratii este infinit dimensional. Conditiile pe care trebuie sa le respecte δ sunt urmatoarele:

1. Pentru orice $(q_1, a_1) \in Q \times A$,
$$\sum_{(q_2,a_2,d)\in Q\times A\times\{-1,0,1\}} |\delta(q_1, a_1, q_2, a_2, d)|^2 = 1.$$
2. Fie C multimea infinita a configuratiilor, $H = \mathbb{C}[C]$ spatiul Hilbert complex generat de C, $U_\delta : H \to H$ functia liniara generata de δ. Atunci U_δ trebuie sa fie unitara.

Pentru o mai buna simulare a masinilor Turing cuantice, se cere ca δ sa ia valori in $\mathbb{Q}[i]$. Nu este clar in ce masura aceasta cerinta restrange conceptul.

Notiunea de masina Turing cuantica fiind foarte complicata, se prefera alte modele de calcul, precum circuitele cuantice.

5 Circuite booleene, reversibile si cuantice

Fixam alfabetul $A = \mathbb{F}_2 = \{0, 1\}$. Se stie ca operatiile $\{\wedge, \vee, \neg\}$ formeaza o famile completa de functii booleene, in sensul ca orice functie $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ se poate defini complet cu ajutorul unui tuplu format din m termeni care contin exact aceste simboluri de functie si variabilele $x_1, \ldots, x_n$.

Un mod mai compact de a reprezenta functiile booleene sunt circuitele booleene. Un **circuit boolean** este un graf aciclic orientat, ale carui varfuri sunt etichetate cu variabile de intrare x_i, variabile de iesire y_j sau operatiile booleene $\wedge$, $\vee$, $\neg$. Conditia este ca varfurile etichetate cu variabile de intrare sa nu primeasca sageti de nicaieri (fanin 0), varfurile etichetate cu variabile de iesire sa primeasca exact o sageata (fanin 1) si sa nu trimita niciuna (fanout 0), varfurile etichetate $\vee$ sau $\wedge$ sa primeasca exact doua sageti si sa trimita cel putin una (fanin 2, fanout ≥ 1) iar varfurile etichetate cu $\neg$ sa primeasca exact o sageata si sa trimita cel putin una (fanin 1, fanout ≥ 1).

O operatie (poarta) **reversibila** este o functie $f : \mathbb{F}_2^m \to \mathbb{F}_2^m$ **bijectiva**.

Exemplu: Functia $T : \mathbb{F}_2^3 \to \mathbb{F}_2^3$, poarta **Toffoli**, data de $T(x_1, x_2, x_3) = (x_1, x_2, x_1x_2 + x_3)$ este o operatie reversibila. □

Exemplu: **Negatia controlata** $N : \mathbb{F}_2^2 \to \mathbb{F}_2^2$ data de $N(x_1, x_2) = (x_1, x_1 + x_2)$ este o operatie reversibila. □

Un **circuit reversibil** este o permutare a lui $\mathbb{F}_2^n$ compusa din operatii reversibile. O multime R de operatii reversibile se numeste **universala** daca orice circuit $C : \mathbb{F}_2^n \to \mathbb{F}_2^n$ se poate construi folosind operatii din R, constante, permutari de bit $(\ldots, x_i, \ldots, x_j, \ldots) \to (\ldots, x_j, \ldots, x_i, \ldots)$ si spatiu aditional. Asta inseamna ca folosind operatiile din R putem construi o permutare $f : \mathbb{F}_2^{n+m} \to \mathbb{F}_2^{m+n}$ astfel incat exista un vector constant $(c_1, \ldots, c_m) \in \mathbb{F}_2^m$ cu proprietatea ca:

$$f(x_1, \ldots, x_n, c_1, \ldots, c_m) = (C(x_1, \ldots, x_n), d_1, \ldots, d_m).$$

Lema: *Operatiile $\{\neg, N, T\}$ formeaza o multime universala de functii reversibile care nu necesita decat constanta* 0.

Demonstratie:

1. Negatia $\neg$ este reversibila, deci poate fi folosita direct.
2. $T(x_1, x_2, 0) = (x_1, x_2, x_1x_2)$, asadar folosind poarta Toffoli putem calcula conjunctia $\wedge$.
3. Fiindca $x_1 \vee x_2 = \neg(\neg x_1 \wedge \neg x_2)$, putem inlocui disjunctiile cu termeni formati din negatii si conjunctii.
4. Pentru a simula situatiile cu fanout > 1 folosim negatia controlata, fiindca $N(x_1, 0) = (x_1, x_1)$ deci se poate duplica primul bit x_1.

□

Teorema: *Poarta Toffoli este o poarta reversibila universala.*

Demonstratie: Deoarece $T(1, 1, x) = (1, 1, \neg x)$ si $T(1, x, y) = (1, x, x + y)$, negatia si negatia controlata se pot simula cu porti Toffoli si constanta 1. □

Identificam stringurile de biti $\vec{x} \in \mathbb{F}_2^m$ cu o baza ortogonala $\{|\vec{x}\rangle \mid \vec{x} \in \mathbb{F}_2^m\}$ a spatiului Hilbert complex H_{2^m} de dimensiune 2^m. Adoptam reprezentarea $|\vec{x}\rangle = \mathrm{e}_i =^T (0, \ldots, 1, \ldots, 0)$, de lungime 2^m, unde $\vec{x}$ este reprezentarea binara a numarului $i + 1$.

Orice operatie reversibila pe m biti se reprezinta in aceasta baza ca matrice de permutare (exact un 1 pe fiecare linie si pe fiecare coloana). Matricea respectiva este unitara si actioneaza ca o operatie cuantica pe H_{2^m}. **Asadar calculabilitatea cuantica generalizeaza calculabilitatea clasica.**

Exemplu: Poarta Toffoli este data de matricea:

$$\begin{pmatrix} I_2 & O & O & O \\ O & I_2 & O & O \\ O & O & I_2 & O \\ O & O & O & M_\neg \end{pmatrix},$$

unde blocurile sunt 2×2, O este matricea nula, I_2 este identitatea iar $M_\neg$ este negatia. Intr-adevar, Toffoli modifica stringul $x_0x_1x_2$ numai in cazurile $110 \to 111$ si $111 \to 110$, adica $\mathrm{e}_7 \to \mathrm{e}_8$ si $\mathrm{e}_8 \to \mathrm{e}_7$. □

6 Caractere de grup

Fie $(G, +, 0)$ un grup abelian. Un **caracter** al lui G este un morfism de grupuri:

$$\chi : (G, +, 0) \to (\mathbb{C} \setminus \{0\}, \cdot, 1).$$

Deci $\chi(0) = 1$. Daca $|G| = n$ este finit, rezulta ca $\chi(g)^n = \chi(ng) = \chi(0) = 1$ asadar valorile lui χ sunt radacini ale unitatii. Daca χ_1 si χ_2 sunt caractere, se observa ca produsul $\chi_1\chi_2$ este si el un caracter. Fie $\hat{G}$ grupul caracterelor, cu acest produs.

Exemplu: Sa calculam $\hat{\mathbb{Z}}_n$. Grupul ciclic $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. Pentru $y \in \mathbb{Z}$ fie:

$$\chi_y(x) = \mathrm{e}^{\frac{2\pi i x y}{n}}.$$

Observam ca χ_y este un caracter al lui $\mathbb{Z}_n$ si ca $\chi_y = \chi_z$ daca si numai daca $y \equiv z \bmod n$. Asadar $\hat{\mathbb{Z}}_n = \{\chi_x \mid x \in \mathbb{Z}_n\} \simeq \mathbb{Z}_n$. □

Se poate arata in general:

Teorema: *Daca G este un grup abelian finit, atunci $G \simeq \hat{G}$.*

Demonstratie: Orice grup abelian finit se scrie ca produs de grupuri ciclice: $G \simeq G_1 \times G_2 \times \cdots \times G_m$. Cum stim ca $\hat{G}_i \simeq G_i$, vrem sa aratam ca $\hat{G} \simeq G$. Dar $G = G_1 \oplus G_2 \oplus \cdots \oplus G_m$, deci orice element $g \in G$ se exprima unic $g = g_1 + \cdots + g_m$, unde $g_i \in G_i$. Fie χ_i un caracter al lui G_i. Definim $\chi : G \to \mathbb{C} \setminus \{0\}$ prin $\chi(g) = \chi_1(g_1) \ldots \chi_m(g_m)$. Se observa ca χ este un caracter al lui G si ca este unic determinat de $\chi_1, \ldots, \chi_m$. □

Aplicatie: Caracterele lui $\mathbb{F}_2^m$. Caracterele lui $(\mathbb{F}_2, +, 0)$ sunt:

$$\chi_y(x) = \mathrm{e}^{\frac{2\pi i x y}{2}} = (-1)^{xy},$$

asadar caracterele lui $\mathbb{F}_2^m$ sunt:

$$\chi_{\vec{y}}(\vec{x}) = (-1)^{x_1y_1 + \cdots + x_my_m} = (-1)^{\vec{x} \cdot \vec{y}}.$$

□

Fie $G = \{g_1, \ldots, g_n\}$ un grup abelian finit. Multimea:

$$\mathbb{V} = \{f : G \to \mathbb{C}\}$$

formeaza un spatiu vectorial peste $\mathbb{C}$. Cum fiecare element este unic determinat de valorile $(f(g_1), \ldots, f(g_n))$, $\mathbb{V}$ are dimensiunea n peste $\mathbb{C}$. O baza este data de functiile e_i cu proprietatea ca $\mathrm{e}_i(g_j) = \delta_{ij}$ adica 1 daca $i = j$ si 0 in caz contrar.

Produsul scalar din spatiul vectorial $\mathbb{V}$ este definit de:

$$\langle f \mid h \rangle = \sum_{i=1}^{n} f^*(g_i) h(g_i).$$

Cu ajutorul lui se defineste norma:

$$\| f \| = \sqrt{\langle f \mid f \rangle}.$$

Teorema de Ortogonalitate a Caracterelor: *Daca χ_i si χ_j sunt caractere ale grupului abelian finit G, atunci:*

$$\langle \chi_i \mid \chi_j \rangle = \begin{cases} 0, & \text{daca } i \neq j, \\ n, & \text{daca } i = j. \end{cases}$$

Demonstratie: Observam ca $1 = |\chi(g)|^2 = \chi^*(g)\chi(g)$, deci $\chi^*(g) = \chi(g)^{-1}$ pentru orice $g \in G$. Deci:

$$\langle \chi_i \mid \chi_j \rangle = \sum_{k=1}^{n} \chi_i^*(g_k)\chi_j(g_k) = \sum_{k=1}^{n} \chi_i^{-1}(g_k)\chi_j(g_k) = \sum_{k=1}^{n} (\chi_i^{-1}\chi_j)(g_k).$$

Daca $i = j$, atunci $\chi_i^{-1}\chi_j$ este caracterul constant 1, si partea a doua rezulta imediat. Daca $i \neq j$ atunci $\chi_i^{-1}\chi_j$ este un caracter netrivial χ si trebuie sa aratam ca pentru un caracter netrivial:

$$S = \sum_{k=1}^{n} \chi(g_k) = 0.$$

Stim ca exista un element $g \in G$ cu $\chi(g) \neq 1$. Aplicatia $g_i \to g_i + g$ este o permutare a lui G deci:

$$S = \sum_{k=1}^{n} \chi(g_k) = \sum_{k=1}^{n} \chi(g + g_k) = \chi(g) \sum_{k=1}^{n} \chi(g_k) = \chi(g)S.$$

Cum $\chi(g) \neq 1$, acest lucru este posibil doar daca $S = 0$. □

De aici rezulta ca functiile:

$$B_i = \frac{1}{\sqrt{n}} \chi_i$$

formeaza o baza a lui $\mathbb{V}$. O alta concluzie este ca matricea $X \in \mathbb{C}^{n \times n}$ cu elemente $\chi_j(g_i)$ are proprietatea:

$$X^{-1} = \frac{1}{n} X^*.$$

7 Transformarea Fourier discreta

Fiecare functie $f \in \mathbb{V}$ are o unica reprezentare conform bazei B data de caracterele grupului G:

$$f = \hat{f}_1 B_1 + \cdots + \hat{f}_n B_n.$$

Functia $\hat{f} : G \to \mathbb{C}$ (adica $\hat{f} \in \mathbb{V}$) definita de relatiile:

$$\hat{f}(g_i) = \hat{f}_i,$$

pentru orice $i = 1$ la n, se numeste **transformata Fourier discreta** a functiei $f \in \mathbb{V}$.
Se observa ca $\langle B_i \mid f \rangle = \hat{f}_i$. Asadar transformata Fourier discreta se poate scrie si ca:

$$\hat{f}(g_i) = \langle B_i \mid f \rangle = \frac{1}{\sqrt{n}} \sum_{k=1}^{n} \chi_i^*(g_k) f(g_k).$$

Exemplu: Transformata Fourier a unei functii $f : \mathbb{Z}_n \to \mathbb{C}$ este:

$$\hat{f}(x) = \frac{1}{\sqrt{n}} \sum_{y \in \mathbb{Z}_n} \mathrm{e}^{-\frac{2\pi i x y}{n}} f(y).$$

□

Exemplu: Transformata Fourier a unei functii $f : \mathbb{F}_2^m \to \mathbb{C}$ este:

$$\hat{f}(\vec{x}) = \frac{1}{\sqrt{2^m}} \sum_{\vec{y} \in \mathbb{F}_2^m} (-1)^{\vec{x} \cdot \vec{y}} f(\vec{y}).$$

Aceasta transformata Fourier se numeste si **transformata Hadamard-Walsh**. □

Observam ca definitia transformatei Fourier discreta poate fi scrisa si:

$$\begin{pmatrix} \hat{f}(g_1) \\ \hat{f}(g_2) \\ \vdots \\ \hat{f}(g_n) \end{pmatrix} = \frac{1}{\sqrt{n}} \begin{pmatrix} \chi_1^*(g_1) & \chi_1^*(g_2) & \dots & \chi_1^*(g_n) \\ \chi_2^*(g_1) & \chi_2^*(g_2) & \dots & \chi_2^*(g_n) \\ \vdots & \vdots & \ddots & \vdots \\ \chi_n^*(g_1) & \chi_n^*(g_2) & \dots & \chi_n^*(g_n) \end{pmatrix} \begin{pmatrix} f(g_1) \\ f(g_2) \\ \vdots \\ f(g_n) \end{pmatrix}.$$

Cum matricea care apare in partea dreapta este X^*, inmultind in partea stanga cu X obtinem:

$$\begin{pmatrix} f(g_1) \\ f(g_2) \\ \vdots \\ f(g_n) \end{pmatrix} = \frac{1}{\sqrt{n}} \begin{pmatrix} \chi_1(g_1) & \chi_2(g_1) & \dots & \chi_n(g_1) \\ \chi_1(g_2) & \chi_2(g_2) & \dots & \chi_n(g_2) \\ \vdots & \vdots & \ddots & \vdots \\ \chi_1(g_n) & \chi_2(g_n) & \dots & \chi_n(g_n) \end{pmatrix} \begin{pmatrix} \hat{f}(g_1) \\ \hat{f}(g_2) \\ \vdots \\ \hat{f}(g_n) \end{pmatrix}.$$

Aceasta relatie justifica urmatoarea definitie. Daca $f : G \to \mathbb{C}$ este o functie, **transformata Fourier inversa** a lui f este functia data de:

$$\tilde{f}(g_i) = \frac{1}{\sqrt{n}} \sum_{k=1}^{n} \chi_k(g_i) f(g_k).$$

Acum este clar ca:

$$\tilde{\hat{f}} = \hat{\tilde{f}} = f.$$

Matricile $\frac{1}{\sqrt{n}}X$ si $\frac{1}{\sqrt{n}}X^*$ sunt unitare, deci conserva $\| \ f \ \|$. Asadar are loc **identitatea lui Parseval**:

$$\| \ \tilde{f} \ \| = \| \ f \ \| = \| \ \hat{f} \ \| \ .$$

Exemple: In $\mathbb{Z}_n$ are loc $\chi_x(y) = \chi_y(x)$ iar transformata Fourier inversa este simetrica cu transformata Fourier:

$$\tilde{f}(x) = \frac{1}{\sqrt{n}} \sum_{y \in \mathbb{Z}_n} \mathrm{e}^{\frac{2\pi i x y}{n}} f(y).$$

In $\mathbb{F}_2^m$ aplicatia Fourier inversa este identica cu aplicatia Fourier directa:

$$\tilde{f}(\vec{x}) = \frac{1}{\sqrt{2^m}} \sum_{y \in \mathbb{F}_2^m} (-1)^{\vec{x} \cdot \vec{y}} f(\vec{y}) = \hat{f}(\vec{x}).$$

□

Functia $f : G \to \mathbb{C}$ se numeste **periodica** daca pentru un $p \in G \setminus \{0\}$ are loc identitatea $f(g + p) = f(g)$ pentru orice $g \in G$. In aceasta situatie:

$$\hat{f}(g_i) = \frac{1}{\sqrt{n}} \sum_{k=1}^{n} \chi_i^*(g_k) f(g_k) = \frac{1}{\sqrt{n}} \sum_{k=1}^{n} \chi_i^*(g_k + p - p) f(g_k + p) =$$

$$= \chi_i^*(-p) \frac{1}{\sqrt{n}} \sum_{k=1}^{n} \chi_i^*(g_k + p) f(g_k + p) = \chi_i^*(-p) \hat{f}(g_i),$$

Dar $\chi_i^*(-p) = \chi_i(-p)^{-1} = \chi_i(p)$. Am aratat:

Propozitie: *Daca functia f este periodica de perioada p iar $\chi_i(p) \neq 1$ atunci $\hat{f}(g_i) = 0$.* □

8 Transformata Fourier cuantica

Fie G un grup abelian finit. Fie H un spatiu Hilbert complex capabil sa reprezinte G. Baza lui H este data de $\{|g\rangle \,|\, g \in G\}$ si contine n elemente. Folosim conventia $|g_i\rangle =^T (0, \ldots, 1, \ldots, 0)$. O stare generala a sistemului cuantic G are forma:

$$c_1|g_1\rangle + \cdots + c_n|g_n\rangle.$$

Ea poate fi privita ca o aplicatie $f : G \to \mathbb{C}$ cu $f(g_i) = c_i$ si $\| f \| = 1$.

Transformata Fourier cuantica (QFT) este aplicatia:

$$\sum_{i=1}^{n} f(g_i)|g_i\rangle \to \sum_{i=1}^{n} \hat{f}(g_i)|g_i\rangle.$$

Dupa cum am vazut, matricea acestei transformari este $\frac{1}{\sqrt{n}}X$, adica:

$$\frac{1}{\sqrt{n}} \begin{pmatrix} \chi_1^*(g_1) & \chi_1^*(g_2) & \cdots & \chi_1^*(g_n) \\ \chi_2^*(g_1) & \chi_2^*(g_2) & \cdots & \chi_2^*(g_n) \\ \vdots & \vdots & \ddots & \vdots \\ \chi_n^*(g_1) & \chi_n^*(g_2) & \cdots & \chi_n^*(g_n) \end{pmatrix},$$

si este o aplicatie unitara din Teorema de Ortogonalitate, respectiv din Identitatea lui Parseval.

In cazul in care $G = U \oplus V$ este o suma directa de grupuri, fiecare element $g \in G$ se scrie unic in forma $g = u + v$ unde $u \in U$ si $v \in V$. In cazul acesta produsul tensorial $H_U \otimes H_V$ reprezinta G cu baza $\{|u\rangle|v\rangle \,|\, u \in U, v \in V\}$. Are loc si descompunerea $\hat{G} = \hat{U} \times \hat{V}$. Prin urmare transformata Fourier cuantica este decompozabila, si produce intotdeauna o stare decompozabila!

Exemplu: Transformata Fourier cuantica a starilor lui $\mathbb{F}_2^m$:

$$|\vec{x}\rangle \to \sum_{\vec{y} \in \mathbb{F}_2^m} (-1)^{\vec{x}\cdot\vec{y}}|y\rangle.$$

Elementele $\vec{x} = (x_1, x_2, \ldots, x_m) \in \mathbb{F}_2^m$ au o reprezentare naturala ca produs tensorial de m qubiti:

$$|\vec{x}\rangle = |x_1\rangle|x_2\rangle \ldots |x_m\rangle.$$

Asadar este suficient sa gasim QFT pentru $\mathbb{F}_2$ si sa aplicam puterea m a produsului tensorial. $\mathbb{F}_2$ cu baza $\{|0\rangle, |1\rangle\}$ are QFT dat de:

$$\begin{aligned} |0\rangle &\to \frac{1}{\sqrt{2}}((-1)^{0\cdot 0}|0\rangle + (-1)^{0\cdot 1}|1\rangle) \\ |1\rangle &\to \frac{1}{\sqrt{2}}((-1)^{1\cdot 0}|0\rangle + (-1)^{1\cdot 1}|1\rangle) \end{aligned}$$

Ne reamintim ca aceasta este matricea Hadamard-Walsh W_2:

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

Matricea Hadamard-Walsh pentre grupul $\mathbb{F}_2^m$ este $W_2^{\otimes m}$. Rezulta ca elementul $\vec{x}\vec{y}$ din matrice este $(1/\sqrt{2})^m(-1)^{\vec{x}\cdot\vec{y}}$. □

Exemplu: Transformata Fourier cuantica a starilor lui $\mathbb{Z}_n$. Daca n este produs $n = n_1 n_2$ cu $\gcd(n_1, n_2) = 1$ atunci $\mathbb{Z}_n \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ si transformata Fourier cuantica QFT este decompozabila in factori mai mici. De aceea este important sa cunoastem comportamentul lui QFT pe grupuri

$\mathbb{Z}_n$ cu $n = p^k$, unde p este numar prim. Un asemenea caz se rezolva complet in exemplul urmator. □

Exemplu: Transformata Fourier cuantica a starilor lui $\mathbb{Z}_{2^m}$. Grupul $\mathbb{Z}_{2^m}$ are o reprezentare naturala folosind m qubiti. Un element $x = x_m 2^{m-1} + x_{m-1}2^{m-2} + \cdots + x_2 2 + x_1$ unde toti $x_i \in \{0, 1\}$, este reprezentat ca:

$$|x\rangle = |x_m\rangle|x_{m-1}\rangle \ldots |x_1\rangle.$$

Cum sa implementam aplicatia QFT **inversa**:

$$|x\rangle \to \frac{1}{\sqrt{2^m}} \sum_{y=0}^{2^m-1} \mathrm{e}^{\frac{2\pi i x y}{2^m}} |y\rangle$$

folosind un circuit cuantic? **Surpriza**: actiunea acestei transformari pe un element de baza este **decompozabila**!

Lema:

$$\sum_{y=0}^{2^m-1} \mathrm{e}^{\frac{2\pi i x y}{2^m}} |y\rangle = (|0\rangle + \mathrm{e}^{\frac{\pi i x}{2^0}}|1\rangle) \ldots (|0\rangle + \mathrm{e}^{\frac{\pi i x}{2^{m-1}}}|1\rangle)$$

Proof: Consideram ultimul qubit din $\vec{y}$: $|\vec{y}\rangle = |\vec{y'}b\rangle = |\vec{y'}\rangle|b\rangle$. Notam $2\pi i x$ cu A. Astfel:

$$\sum_{y=0}^{2^m-1} \exp\Big(\frac{Ay}{2^m}\Big)|y\rangle = \sum_{y'=0}^{2^{m-1}-1} \exp\Big(\frac{A \cdot 2y'}{2^m}\Big)|y'0\rangle + \sum_{y'=0}^{2^{m-1}-1} \exp\Big(\frac{A(2y'+1)}{2^m}\Big)|y'1\rangle =$$

$$= \sum_{y=0}^{2^{m-1}-1} \exp\Big(\frac{A \cdot 2y}{2^m}\Big)|y\rangle|0\rangle + \sum_{y=0}^{2^{m-1}-1} \exp\Big(\frac{A \cdot 2y}{2^m}\Big) \exp\Big(\frac{A}{2^m}\Big)|y\rangle|1\rangle =$$

$$\sum_{y=0}^{2^{m-1}-1} \exp\Big(\frac{2\pi i x y}{2^{m-1}}\Big)|y\rangle\Big(|0\rangle + \exp\Big(\frac{\pi i x}{2^{m-1}}\Big)|1\rangle\Big).$$

Prin inductie sunt transformati toti qubitii de la dreapta la stanga. □

Se observa ca faza l a lui $|1\rangle$ depinde numai de bitii $x_1, \ldots, x_l$. Mai exact:

$$\exp\Big(\pi i \frac{2^m x_m + \cdots + x_1}{2^{l-1}}\Big) = \exp\Big(\pi i \frac{2^l x_l + \cdots + x_1}{2^l}\Big) =$$

$$= \exp\Big(\frac{\pi i x_l}{2^0}\Big) \exp\Big(\frac{\pi i x_{l-1}}{2^1}\Big) \cdot \cdots \cdot \exp\Big(\frac{\pi i x_2}{2^{l-1}}\Big) \exp\Big(\frac{\pi i x_1}{2^l}\Big) =$$

$$= (-1)^{x_l} \exp\Big(\frac{\pi i x_{l-1}}{2^1}\Big) \cdot \cdots \cdot \exp\Big(\frac{\pi i x_2}{2^{l-2}}\Big) \exp\Big(\frac{\pi i x_1}{2^{l-1}}\Big).$$

Acum descriem circuitul cuantic care produce actiunea lui QFT pe elementele de baza ale lui $\mathbb{Z}_{2^m}$, adica pe elementele:

$$|\vec{x}\rangle = |x_1\rangle|x_2\rangle \ldots |x_m\rangle.$$

1. Se actioneaza cu transformarea Hadamard-Walsh qubitul m. Se obtine:

$$\frac{1}{\sqrt{2}}|x_1\rangle|x_2\rangle \ldots |x_{m-2}\rangle(|0\rangle + (-1)^{x_m}|1\rangle).$$

2. Se completeaza faza $(-1)^m$ la faza:

$$(-1)^m \exp\Big(\frac{2\pi i x_{m-1}}{2^2}\Big) \ldots \exp\Big(\frac{2\pi i x_2}{2^{m-1}}\Big) \exp\Big(\frac{2\pi i x_1}{2^m}\Big).$$

folosind rotatiile respective in mod **conditionat**: o rotatie se aplica daca si numai daca atat bitul x_m cat si bitul x_i sunt 1.

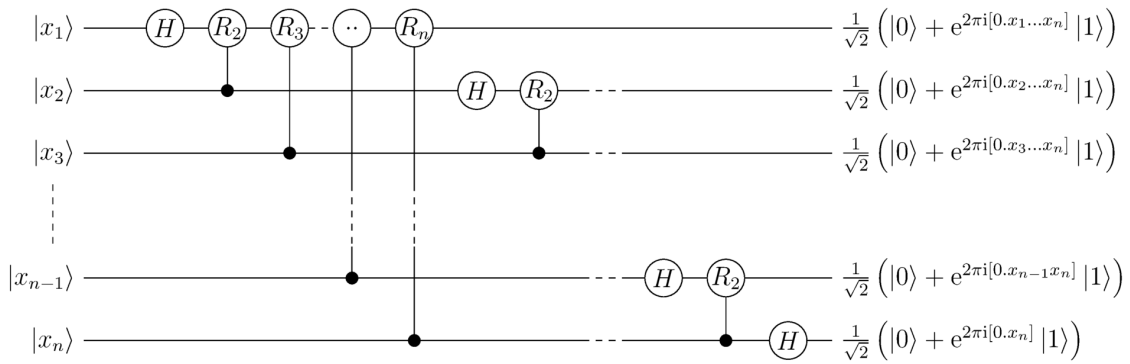

Figure 1: Circuit cuantic pentru QFT. Sursa: Wikipedia.

3. Pasii 1. si 2. se repeta succesiv pentru ceilalti biti: $m-2, \ldots, 0$.

Daca R_k este rotatia:

$$\begin{pmatrix} 1 & 0 \\ 0 & \exp\left(\frac{2\pi i}{2^k}\right) \end{pmatrix}$$

atunci circuitul cuantic arata ca in figura. Starea de iesire este produsul tensorial al qubitilor din portile de iesire.

9 De la perioade la factorizare

Fie $n = p_1^{e_1} \ldots p_k^{e_k}$ descompunerea in factori primi (necunoscuta!) a unui numar impar. Cum exista un algoritm clasic in timp polinomial care decide daca un numar este putere perfecta de numar natural (Exercitiu!) presupunem $k \geq 2$. Dorim sa gasim un divizor netrivial d al lui n. Daca putem face asta, atunci putem repeta algoritmul pentru d si n/d, si in scurt timp aflam descompunerea in factori primi a lui n.

Se alege la intamplare, cu probabilitate uniforma, $a \in \mathbb{Z}_n$ cu $a \neq 0$ si $a \neq 1$. Daca $d = \gcd(n, a) > 1$ atunci d este un divizor al lui n si suntem gata. Numarul d s-ar calcula cu algoritmul lui Euclid. Daca $d = 1$ atunci a apartine grupului unitatilor multiplicative $\mathbb{Z}_n^\times$. Presupunem ca putem afla usor $r = \mathrm{ord}_n(a)$, adica ordinul elementului a in grupul multiplicativ $\mathbb{Z}_n^\times$. Deci:

$$a^r \equiv 1 \bmod n,$$

adica $n \mid a^r - 1$. Daca r este par, atunci $n \mid (a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} + 1)$, deci ar avea factor comun cu cel putin unul dintre ele, si acest factor s-ar gasi cu algoritmul lui Euclid. Ce se intampla insa daca $n \mid (a^{\frac{r}{2}} \pm 1)$ si factorul obtinut este chiar n? Acest lucru este foarte improbabil, dupa cum urmeaza:

In primul rand, daca $n \mid (a^{\frac{r}{2}} - 1)$ atunci :

$$a^{\frac{r}{2}} \equiv 1 \bmod n,$$

ceea ce contrazice definitia ordinului.

In al doilea rand, s-ar putea ca $n \mid (a^{\frac{r}{2}} + 1)$ si in acelasi timp $\gcd(n, a^{\frac{r}{2}} - 1) = 1$. Din prima relatie obtinem:

$$a^{\frac{r}{2}} \equiv -1 \bmod n.$$

In sectiunea urmatoare vom arata ca **probabilitatea** ca ordinul lui a sa fie par si ca $a^{\frac{r}{2}} \not\equiv -1 \bmod n$ este cel putin 9/16.

Deci presupunand ca $\mathrm{ord}_n(a)$ poate fi calculat repede, se poate gasi un factor al lui n in putine incercari. Peste doua sectiuni vom arata ca ordinul se calculeaza rapid folosind un circuit cuantic.

Exemplu: $15 = 3 \cdot 5$ este cel mai mic numar care se poate factoriza prin aceasta metoda.

$$\mathbb{Z}_{15}^{\times} = \{1, 2, 4, 7, 8, 11, 13, 14\}.$$

iar ordinele elementelor sunt 0, 4, 2, 4, 4, 2, 4, 2. Singurul element pentru care $a^{\frac{r}{2}} \equiv -1 \bmod 15$ este $a = 14$. Pentru $a = 7$, $7^2 - 1 \equiv 3 \bmod 15$ iar $7^2 + 1 \equiv 5 \bmod 15$. Atat 3 cat si 5 sunt factori ai lui 15. □

10 Ordin modulo n

Fie $n = p_1^{e_1} \dots p_k^{e_k}$ un numar impar cu descompunerea lui in factori primi, $k \geq 2$. Fie $a \in \mathbb{Z}_n^{\times}$ un element ales la intamplare. Din Teorema Chineza a Resturilor,

$$\mathbb{Z}_n^{\times} = \mathbb{Z}_{p_1^{e_1}}^{\times} \times \dots \times \mathbb{Z}_{p_k^{e_k}}^{\times},$$

deci grupul $\mathbb{Z}_n^{\times}$ este un produs direct de grupuri ciclice. Cardinalitatea fiecarui factor este $\varphi(p_i^{e_i}) = p_i^{e_i - 1}(p_i - 1)$ si este in particular un numar par. Elementul a corespunde unui tuplu:

$$(a_1, \dots, a_k) \in \mathbb{Z}_{p_1^{e_1}}^{\times} \times \dots \times \mathbb{Z}_{p_k^{e_k}}^{\times}.$$

Ordinul elementului $a \in \mathbb{Z}_{p^e}$ se noteaza $\mathrm{ord}_{p^e}(a)$.

Lema: *Fie $\varphi(p^e) = 2^u v$ unde $u \geq 1$, $2 \not| v$ si $s \geq 0$ este fixat. Atunci probabilitatea ca pentru un element ales la intamplare $a \in \mathbb{Z}_{p^e}^{\times}$, $\mathrm{ord}_{p^e}(a) = 2^s t$ unde $2 \not| t$, este $\leq \frac{1}{2}$.*

Demonstratie: Daca $s > u$, probabilitatea este 0. Deci fie $s \leq u$. Ne reamintim ca grupul unitatilor lui $\mathbb{Z}_n$ este ciclic numai pentru $n \in \{2, 4, p^e, 2p^e\}$. Fie g un generator al grupului $\mathbb{Z}_{p^e}^{\times}$. Grupul $\mathbb{Z}_{p^e}^{\times} = \{g^0, g^1, \dots, g^{2^u v - 1}\}$ si:

$$\mathrm{ord}(g^j) = \frac{2^u v}{\gcd(j, 2^u v)},$$

deci ordinul $2^s t$ apare numai daca $j = 2^{u-s} w$ unde $2 \not| w$. In multimea $\{0, 1, 2, \dots, 2^u v - 1\}$ sunt exact $2^s v$ multipli de 2^{u-s} si anume $1 \cdot 2^{u-s}, \dots, (2^s v - 1)2^{u-s}$, dar numai jumatate dintre ei au coeficient impar. Deci probabilitatea este:

$$\frac{\frac{1}{2} \cdot 2^s v}{2^u v} = \frac{2^s}{2^{u+1}} \leq \frac{1}{2}.$$

□

Lema: *Pentru $a \in \mathbb{Z}_n^{\times}$, probabilitatea ca $\mathrm{ord}_n(a)$ sa fie impar este cel mult 2^{-k}.*

Demonstratie: Fie $(a_1, \dots, a_k)$ descompunerea lui a conform Teoremei Chineze a Resturilor. Fie $r_i = \mathrm{ord}_{p_i^{e_i}}(a_i)$. Cum $r = \mathrm{lcm}(r_1, \dots, r_k)$, r este impar daca si numai daca toti r_i sunt impari. Aceasta probabilitate este de cel mult $(1/2) \dots (1/2) = 2^{-k}$. □

Lema: *Pentru $n = p_1^{e_1} \dots p_k^{e_k}$ impar cu $k \geq 2$, daca $r = \mathrm{ord}_n(a)$ este par, probabiliatea ca $a^{\frac{r}{2}} \equiv -1 \bmod n$ este cel mult 2^{-k}.*

Demonstratie: Congruenta $a^{\frac{r}{2}} \equiv -1 \bmod n$ implica $a^{\frac{r}{2}} \equiv -1 \bmod p_i^{e_i}$ pentru toti i. Fie r ordinul lui a modulo n iar r_i ordinul lui a modulo $p_i^{r_i}$. Fie $r = 2^s t$ si $r_i = 2^{s_i} t_i$, unde $2 \not| t$ si $2 \not| t_i$. Cum toti $r_i | r$ pentru toti i, rezulta $s_i \leq s$, dar congruentele au loc doar daca $s_i = s$ pentru toti i.

Intr-adevar, daca $s_i < s$ atunci $r_i | \frac{r}{2}$ (deoarece $k \geq 2$) ceea ce implica $a^{\frac{r}{2}} \equiv 1 \bmod p_i^{e_i}$. Dar asta ar implica $1 \equiv -1 \bmod p_i^{e_i}$, ceea ce nu se poate fiindca $p_i \neq 2$. Asadar probabilitatea in cauza este $\leq$ decat probabilitatea ca $s_i = s$ pentru toti i, care este $\leq (1/2) \ldots (1/2) = 2^{-k}$. □

Punand aceste leme cap la cap obtinem urmatoarea:

Teorema: *Fie $n = p_1^{e_1} \ldots p_k^{e_k}$ impar cu $k \geq 2$. Pentru $a \in \mathbb{Z}_n^\times$ ales la intamplare, probabilitatea ca $\mathrm{ord}_n(a)$ sa fie par si ca $a^{\frac{r}{2}} \not\equiv -1 \bmod n$ este de cel putin $(1 - 2^{-k})^2 \geq \frac{9}{16}$.* □

11 Algoritm cuantic pentru aflarea ordinului

Am aratat deja o legatura intre perioada unei functii discrete si transformarea Fourier discreta. Cum nu putem calcula transformarea Fourier cuantica peste tot $\mathbb{Z}$, alegem un domeniu $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ cu $m > n$ suficient de mare ca o perioada sa poata aparea. Alegem $m = 2^l$ pentru ca putem calcula QFT pentru $\mathbb{Z}_{2^l}$. Valoarea lui l va fi fixata mai tarziu. $\mathbb{Z}_m$ are nevoie de l qubiti iar $\mathbb{Z}_n$ are nevoie de cel mult l qubiti. Pentru reprezentare vom folosi notatia $|x\rangle|y\rangle$ cu $x \in \mathbb{Z}_m$ si $y \in \mathbb{Z}_n$.

1. Se porneste cu starea $|0\rangle|0\rangle$ si se aplica Hadamard-Walsh pe primul $|0\rangle$. Rezulta:

$$\frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |k\rangle|0\rangle.$$

2. Se calculeaza $k \to a^k \bmod n$ folosind un circuit booleean mic, care este simulat de un circuit cuantic mic. Se obtine superpozitia:

$$\frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |k\rangle|a^k\rangle.$$

   Fiindca functia $k \to a^k \bmod n$ are perioada $\mathrm{ord}_n(a) = r$, superpozitia poate fi scrisa in forma:

$$\frac{1}{\sqrt{m}} \sum_{l=0}^{r-1} \sum_{q=0}^{s_l} |qr + l\rangle|a^l\rangle,$$

   unde s_l este cel mai mare intreg pentru care $s_l r + l < m$. El se determina cu inegalitatile:

$$\frac{m}{r} - 1 - \frac{l}{r} \leq s_l < \frac{m}{r} - \frac{l}{r}.$$

3. Se calculeaza aplicatia QFT inversa pe $\mathbb{Z}_m$ si se obtine:

$$\frac{1}{\sqrt{m}} \sum_{l=0}^{r-1} \sum_{q=0}^{s_l} \frac{1}{\sqrt{m}} \sum_{p=0}^{m-1} \exp\Big(\frac{2\pi i p(qr+l)}{m}\Big)|p\rangle|a^l\rangle =$$

$$= \frac{1}{m} \sum_{l=0}^{r-1} \sum_{p=0}^{m-1} \exp\Big(\frac{2\pi i p l}{m}\Big) \sum_{q=0}^{s} \exp\Big(\frac{2\pi i p r q}{m}\Big)|p\rangle|a^l\rangle.$$

4. Se considera aceasta superpozitie ca reprezentare a lui $\mathbb{Z}_m$. Se face o observatie si se citeste un $p \in \mathbb{Z}_m$.

5. Se considera numarul rational $\frac{p}{m}$. Se calculeaza convergentii $\frac{p_i}{q_i}$. Se gaseste cel mai mic q_i astfel incat $a^{q_i} \equiv 1 \bmod n$, daca el exista.

Explicatie: Consideram fractia ireductibila $\frac{263}{189}$. Algoritmul lui Euclid genereaza urmatoarea demonstratie:

$$\begin{aligned} 263 &= 1 \cdot 189 + 74, \\ 189 &= 2 \cdot 74 + 41, \\ 74 &= 1 \cdot 41 + 33, \\ 41 &= 1 \cdot 33 + 8, \\ 33 &= 4 \cdot 8 + 1. \end{aligned}$$

Transpus in numere rationale, asta se scrie in modul urmator:

$$\begin{aligned} \frac{263}{189} &= 1 + \frac{74}{189}, \\ \frac{189}{74} &= 2 + \frac{41}{74}, \\ \frac{74}{41} &= 1 + \frac{33}{41}, \\ \frac{41}{33} &= 1 + \frac{8}{33}, \\ \frac{33}{8} &= 4 + \frac{1}{8}, \end{aligned}$$

ceea ce permite urmatoarea reprezentare ca fractie continua:

$$\frac{263}{189} = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \frac{1}{8}}}}}.$$

Daca fractia continua se noteaza $[a_0, a_1, a_2, \ldots, a_n]$, in cazul nostru $[1, 2, 1, 1, 4, 8]$, convergentii sunt fractiile $\frac{p_i}{q_i}$ unde:

$$\frac{p_0}{q_0} = \frac{a_0}{1}, \quad \frac{p_1}{q_1} = \frac{a_0 a_1 + 1}{a_1},$$
$$\frac{p_i}{q_i} = \frac{a_i p_{i-1} + p_{i-2}}{a_i q_{i-1} + q_{i-2}}.$$

In cazul nostru convergentii sunt:

$$1, \frac{3}{2}, \frac{4}{3}, \frac{7}{5}, \frac{32}{23}, \frac{263}{189}.$$

□

Exemplu: Fie $n = 15$ si $a = 7$ elementul al carui ordin trebuie calculat. Alegem $m = 16$.

1. Se prepara starea:
$$\frac{1}{4} \sum_{k=1}^{15} |k\rangle|0\rangle.$$

2. Puterile $k \to 7^k \bmod 15$ produc starea:
$$\frac{1}{4}\Big(|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + |3\rangle|13\rangle + |4\rangle|1\rangle + \cdots + |15\rangle|13\rangle\Big) =$$
$$= \frac{1}{4}(|0\rangle + |4\rangle + |8\rangle + |12\rangle)|1\rangle +$$

$$+\frac{1}{4}(|1\rangle + |5\rangle + |9\rangle + |13\rangle)|7\rangle +$$
$$+\frac{1}{4}(|2\rangle + |6\rangle + |10\rangle + |14\rangle)|4\rangle +$$
$$+\frac{1}{4}(|3\rangle + |7\rangle + |11\rangle + |15\rangle)|13\rangle.$$

3. Aplicatia QFT inversa pe $\mathbb{Z}_{16}$ da:

$$= \frac{1}{4}(|0\rangle + |4\rangle + |8\rangle + |12\rangle)|1\rangle +$$
$$+\frac{1}{4}(|0\rangle + i|4\rangle - |8\rangle - i|12\rangle)|7\rangle +$$
$$+\frac{1}{4}(|0\rangle - |4\rangle + |8\rangle - |12\rangle)|4\rangle +$$
$$+\frac{1}{4}(|0\rangle - i|4\rangle - |8\rangle + i|12\rangle)|13\rangle.$$

4. Probabilitatea de a observa elementele 0, 4, 8, 12 este 1/4 pentru fiecare.

5. Singurul convergent al lui 0 este 0, si el nu da perioada. Convergentii lui 4/16 sunt 0/1 si 1/4, iar al doilea da perioada corecta 4. Observarea lui 8 produce convergentii lui 8/16 care sunt 0/1 si 1/2, si nu produc perioada. Dar observarea lui 12 duce la convergentii lui 12/16, care sunt 0/1, 1/1 si 3/4. Ultimul produce perioada (ordinul lui 7.)

12 Probabilitatea de succes

Probabilitatea observarii unui anumit $p \in \mathbb{Z}_m$ este:

$$P(p) = \sum_{l=0}^{r-1} \frac{1}{m^2} \Big| \exp\big(\frac{2\pi ipl}{m}\big) \sum_{q=0}^{s_l} \exp\big(\frac{2\pi ipqr}{m}\big) \Big|^2 = \frac{1}{m^2} \sum_{l=0}^{r-1} \Big| \sum_{q=0}^{s_l} \exp\big(\frac{2\pi ipqr}{m}\big) \Big|^2.$$

Vom arata ca aceasta observatie duce la calculul perioadei cu o probabilitate importanta.

Pentru inceput tratam **cazul usor** in care $r \mid m$. Cum s_l este cel mai mare intreg astfel incat $s_l r + l < m$ unde $0 \le l < r$, se observa ca pentru toti l are loc $s_l = m/r - 1$. In acest caz:

$$P(p) = \frac{r}{m^2} \Big| \sum_{q=0}^{m/r-1} \exp\big(\frac{2\pi ipq}{m/r}\big) \Big|^2.$$

Din proprietatea de ortogonalitate a caracterelor stim ca:

$$\sum_{q=0}^{m/r-1} \exp\big(\frac{2\pi ipq}{m/r}\big) = \begin{cases} \frac{m}{r}, & \text{daca } p = 0 \text{ in } \mathbb{Z}_{m/r}, \\ 0, & \text{altfel.} \end{cases}$$

$$P(p) = \begin{cases} \frac{1}{r}, & \text{daca } p = 0 \text{ in } \mathbb{Z}_{m/r}, \\ 0, & \text{altfel.} \end{cases}$$

Deci in cazul in care $r \mid m$ observatia poate produce doar un p in multimea $\{0, m/r, 2m/r, \ldots, (r-1)m/r\}$, fiecare cu probabilitate $1/r$. Obtinem rezolventul bun cu siguranta numai daca $\gcd(d, r) = 1$. Vom vedea ca probabilitatea acestui eveniment nu tinde la 0 decat suficient de incet.

Cu aceste pregatiri, putem ataca **cazul general**.

Avand in vedere ca $m = 2^l$, in general r nu divide m. Totusi, putem intreba care este probabilitatea sa observam un p apropiat de un multiplu al lui $\frac{m}{r}$. Daca numarul:

$$m\Big|\frac{p}{m} - \frac{d}{r}\Big| = \Big|p - d\frac{m}{r}\Big|$$

este suficient de mic si $\gcd(d, r) = 1$ atunci $\frac{d}{r}$ este un convergent al lui $\frac{p}{m}$ iar convergentii se gasesc eficient cu algoritmul lui Euclid.

Cautam un m astfel incat metoda fractiilor continue se aplica. Pentru orice $d \in \{0, 1, \ldots, r-1\}$ exista un unic intreg p astfel incat inegalitatea:

$$-\frac{1}{2} < p - d\frac{m}{r} \leq \frac{1}{2}$$

are loc. Daca alegem m astfel incat $n^2 \leq m$, atunci:

$$\Big|\frac{p}{m} - \frac{d}{r}\Big| \leq \frac{1}{2m} \leq \frac{1}{2n^2} < \frac{1}{2r^2}.$$

Aici se poate aplica o Teorema cunoscuta din Algebra:

Teorema: *Daca*

$$0 < \Big|\frac{p}{q} - \alpha\Big| \leq \frac{1}{2q^2},$$

atunci atunci $\frac{p}{q}$ este un convergent al expansiunii lui α in fractie continua. □

Datorita acestei Teoreme obtinem ca daca $\gcd(d, r) = 1$ atunci $\frac{d}{r}$ este un convergent al lui $\frac{p}{m}$.

Dar sunt numai r intregi $p \in \mathbb{Z}_m$ care satisfac aceasta inegalitate, si anume cate unul pentru fiecare $d \in \{0, 1, \ldots, r-1\}$. Care este probabilitatea sa il observam pe unul dintre ei? Cu alte cuvinte, care este probabilitatea sa se observe un $p \in \mathbb{Z}_m$ astfel incat exista un $d \in \{0, 1, \ldots, r-1\}$ si sa aiba loc:

$$|pr - dm| \leq \frac{r}{2}.$$

Lema: *Pentru $n \geq 100$, observatia circuitului cuantic va da un $p \in \mathbb{Z}_m$ astfel incat pentru un $0 \leq d \leq r-1$, are loc $|pr - dm| \leq \frac{r}{2}$ cu o probabilitate $\geq \frac{2}{5}$.*

Demonstratie: Intai avem in vedere urmatoarele exercitii:

Exercitiul 1: $|\exp(ix) - 1|^2 = 4\sin^2\frac{x}{2}$.

Exercitiul 2:

$$\Big|\sum_{q=0}^{s} \exp\big(\frac{2\pi ipqr}{m}\big)\Big|^2 = \frac{\sin^2\frac{\pi pr(s+1)}{m}}{\sin^2\frac{\pi pr}{m}}.$$

Datorita acestei estimari,

$$P(p) = \frac{1}{m^2}\sum_{l=0}^{r-1} \frac{\sin^2\frac{\pi pr(s_l+1)}{m}}{\sin^2\frac{\pi pr}{m}} = \frac{1}{m^2}\sum_{l=0}^{r-1} \frac{\sin^2\frac{\pi(pr-dm)(s_l+1)}{m}}{\sin^2\frac{\pi(pr-dm)}{m}},$$

pentru orice d fixat, din periodicitatea lui sin^2x. De acum incolo $x = pr - dm$ ia valori in intervalul $[-\frac{r}{2}, \frac{r}{2}]$. Pe acest interval vom estima functia:

$$f(x) = \frac{\sin^2\frac{\pi x(s_l+1)}{m}}{\sin^2\frac{\pi x}{m}}.$$

Functia f este o functie para, ia maximul $(s_l+1)^2$ in $x = 0$ si minimul in punctele $\pm\frac{r}{2}$. Deci:

$$f(x) \geq \frac{\sin^2\frac{\pi r(s_l+1)}{2m}}{\sin^2\frac{\pi r}{2m}}.$$

Cum s_l este cel mai mare intreg astfel incat $s_l r + l < m$, au loc inegalitatile:

$$\frac{\pi}{2}\Big(1 - \frac{r}{m}\Big) < \frac{\pi r}{2m}\Big(s_l + 1\Big) < \frac{\pi}{2}\Big(1 + \frac{r}{m}\Big),$$

deci:

$$f(x) \geq \frac{\sin^2 \frac{\pi}{2}\big(1 - \frac{r}{m}\big)}{\sin^2 \frac{\pi r}{2m}}.$$

Prin alegerea lui $m \geq n^2$, $\frac{m}{r}$ este neglijabila, si putem folosi estimarile $\sin x \leq x$ si $\sin^2 \frac{\pi}{2}(1+x) \geq 1 - (\frac{\pi}{2}x)^2$ pentru a obtine:

$$f(x) \geq \frac{4}{\pi^2}\Big(\frac{m}{r}\Big)^2\Big(1 - \big(\frac{\pi}{2}\frac{r}{m}\big)^2\Big),$$

deci:

$$P(p) \geq \frac{4}{\pi^2}\frac{1}{r}\Big(1 - \big(\frac{\pi}{2}\frac{r}{m}\big)^2\Big).$$

Dar factorul:

$$\Big(1 - \big(\frac{\pi}{2}\frac{r}{m}\big)^2\Big)$$

tinde la 1 cand $r/m \to 0$ iar pentru $n \geq 100$ este deja mai mare decat 0.9999. Deci probabilitatea de a observa un p fixat este de cel putin $\frac{2}{5}\frac{1}{r}$ pentru orice $n \geq 100$.

Dar sunt exact r asemenea valori p. Probabilitatea de a observa unul dintre ei este $\geq \frac{2}{5}$. □

Prin urmare fiecare d corespunzator unui asemenea p se obtine cu o probabilitate de $\frac{2}{5r}$. Acum vom estima cu ce probabilitate, pentru un asemenea d, are loc $\gcd(d, r) = 1$. Probabilitatea ca $\gcd(d, r) = 1$ pentru $d \in \{0, 1, \ldots, r-1\}$ este $\varphi(r)/r$. Ea poate fi estimata folosind urmatorul rezultat:

Teorema: *Pentru $r \geq 3$,*

$$\frac{r}{\varphi(r)} < \mathrm{e}^{\gamma} \log\log r + \frac{2.50637}{\log\log r},$$

unde $\gamma = 0.5772156649\cdots = \lim_{n\to\infty}(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log n)$ este constanta lui Euler.

Asta implica:

Lema: *Pentru $r \geq 19$, probabilitatea ca $d \in \{0, 1, \ldots, r-1\}$ sa aiba loc $\gcd(d, r) = 1$, este de cel putin $\frac{1}{4 \log\log n}$.*

Daca combinam toate aceste rezultate, aflam ca probabilitatea ca algoritmul cuantic sa afle ordinul unui element din $\mathbb{Z}_n$ este de cel putin:

$$\frac{9}{160}\frac{1}{\log\log n}.$$

Algoritmul cuantic al lui Shor

Input: $n \in \mathbb{N}$ impar, compus.

Output: Factor netrivial al lui n.

1. Alege $a \in \{1, 2, \ldots, n-1\}$ la intamplare.
2. Calculeaza $d = \gcd(a, n)$ cu algoritmul lui Euclid. Daca $d > 1$, afiseaza d si **stop**.
3. Calculeaza r cu algoritmul cuantic, unde $m = 2^l$ este ales astfel incat $n^2 < m$. Daca $a^r \not\equiv 1 \bmod n$ sau r este impar sau $a^{\frac{r}{2}} \equiv -1 \bmod n$, calculeaza un alt r.
4. Calculeaza $d_{\pm} = \gcd(n, a^{\frac{r}{2}} \pm 1)$. Afiseaza $d_{\pm}$ si **stop**.

Fie $l(n)$ lungimea binara a numarului n. Algoritmul lui Euclid are nevoie de $O(l(n)^3)$. Transformarea Hadamard are nevoie de $O(l(n))$, $a^k \bmod n$ se face in $O(l(n)^3)$, QFT se face in $O(l(n)^2)$, iar calculul convergentilor in timp $O(l(n)^3)$. La sfarsit se mai face un Euclid, timp $O(l(n)^3)$. Dar probabilitatea este $\Omega(\frac{1}{\log\log n}) = \Omega(\frac{1}{\log l(n)})$, daca repetam algoritmul $O(\log l(n))$ ori se extrage factorizarea in timp $O(l(n)^3 \log l(n))$ cu mare probabilitate.

13 Problema subgrupului ascuns

Input: G grup abelian finit, $\rho : G \to R$, R finita. Se presupune ca exista un subgrup $H \leq G$ astfel incat ρ e constanta pe fiecare clasa xH.

Output: Multime de generatori pentru H.

Vom trata cazul $G = \mathbb{F}_2^m$.

Lema: *Daca $\vec{y} \in \mathbb{F}_2^m$ si $H \leq \mathbb{F}_2^m$ subgrup, atunci:*

$$\sum_{\vec{h} \in H} (-1)^{\vec{h}\cdot\vec{y}} = \begin{cases} |\, H \,| & \vec{y} \in H^\perp, \\ 0 & \text{altfel.} \end{cases}$$

Demonstratie: Daca $\vec{y} \in H^\perp$ si $\vec{h} \in H$, atunci $\vec{y} \cdot \vec{h} = 0$. OK.

Daca $\vec{y} \notin H^\perp$ atunci exista $\vec{h}_1 \in H$ cu $\vec{y} \cdot \vec{h}_1 \neq 0$. Deci:

$$S = \sum_{\vec{h} \in H} (-1)^{\vec{h}\cdot\vec{y}} = \sum_{\vec{h} \in H} (-1)^{(\vec{h}+\vec{h}_1)\cdot\vec{y}} = (-1)^{\vec{h}_1\cdot\vec{y}} S = -S,$$

deci $S = 0$. □

Definitie: O multime $T \subset G$ se numeste *transversala* a lui H daca pentru orice clasa xH, $xH \cap T$ are un singur element.

Cum $|\, T \,| = [\mathbb{F}_2^m : H]$ si $H \times H^\perp = \mathbb{F}_2^m$ rezulta ca $|\, T \,| = |\, H^\perp \,|$.

Codificam elementele lui $\mathbb{F}_2^m$ prin m qubiti si valorile functiei ρ prin $\log_2[\mathbb{F}_2^m : H] = m - \log_2 |\, H \,|$ qubiti. Se presupune ca ρ e calculabila in timp polinomial. Daca avem o baza Y a lui $H^\perp$, se calculeaza o baza X a lui H prin algoritmul Gauss-Jordan. (polinomial)

ALGORITM A (gasirea unei baze daca dimensiunea d este cunoscuta)

1. Daca $d = \dim H^\perp = 0$ output $\emptyset$.
2. Folositi algoritmul B pentru a alege $Y \subset H^\perp$ cu $|\, Y \,| = d$ **uniform**.
3. Daca Y este liniar independenta, output Y. Altfel output **error**.

Vom vedea ca probabilitatea de a alege o baza este $> \frac{1}{4}$ deci acest algoritm se repeta de 4 - 5 ori.

ALGORITM B (alegerea uniforma a elementelor din $H^\perp$)

1. Folosind Hadamard-Walsh se prepara superpozitia:
$$\frac{1}{\sqrt{2^m}} \sum_{x \in \mathbb{F}_2^m} |x\rangle|0\rangle.$$
2. Calculam ρ. Obtinem superpozitia:
$$\frac{1}{\sqrt{2^m}} \sum_{x \in \mathbb{F}_2^m} |x\rangle|\rho(x)\rangle = \frac{1}{\sqrt{2^m}} \sum_{t \in T} \sum_{x \in H} |T + x\rangle|\rho(t)\rangle.$$

3. Use the Hadamard-Walsh transform on $\mathbb{F}_2^m$ to get:

$$\frac{1}{\sqrt{2^m}}\sum_{t\in T}\sum_{x\in H}\frac{1}{\sqrt{2^m}}\sum_{y\in\mathbb{F}_2^m}(-1)^{(t+x)\cdot y}|y\rangle|\rho(t)\rangle =$$

$$= \frac{1}{\sqrt{2^m}}\sum_{t\in T}\sum_{y\in\mathbb{F}_2^m}(-1)^{t\cdot y}\sum_{x\in H}(-1)^{x\cdot y}|y\rangle|\rho(t)\rangle =$$

$$= \frac{|\,H\,|}{\sqrt{2^m}}\sum_{t\in T}\sum_{y\in H^\perp}(-1)^{t\cdot y}|y\rangle|\rho(t)\rangle.$$

4. Se observa un element $y \in H^\perp$.

Se observa ca:

$$P(y) = \frac{|\,T\,||\,H\,|^2}{2^{2m}} = \frac{1}{|\,H^\perp\,|},$$

deci alegerea este uniforma. Vom vedea ca numarul de incercari este marginit:

Lema: *Fie $t \le d$ si $y_1, y_2, \ldots, y_d \in \mathbb{V}$ alesi uniform, unde $\mathbb{V}$ este spatiu vectorial de dimensiune d peste $\mathbb{F}_2$. Atunci probabilitatea ca acesti vectori sa fie liniar independenti este cel putin $\frac{1}{4}$.*

Demonstratie: Probabilitatea este:

$$p = \frac{2^d-2^0}{2^d}\frac{2^d-2^1}{2^d}\cdots\frac{2^d-2^{t-1}}{2^d}.$$

$$\frac{1}{p} = \prod_{i=0}^{t-1}\frac{2^d}{2^d-2^i} = \prod_{i=0}^{t-1}\frac{2^{d-i}}{2^{d-i}-1} = \prod_{i=1}^{t}\frac{2^{d-t+i}}{2^{d-t+i}-1} \le \prod_{i=1}^{t}\frac{2^i}{2^i-1} = 2\prod_{i=2}^{t}(1+\frac{1}{2^i-1}).$$

Rezulta ca:

$$\ln\frac{1}{2p} \le \sum_{i=2}^{t}\ln(1+\frac{1}{2^i-1}) \le \sum_{i=2}^{t}\frac{1}{2^i-1} \le \sum_{i=2}^{t}\frac{1}{\frac{3}{4}\cdot 2^i} < \frac{4}{3}\sum_{i=2}^{\infty}\frac{1}{2^i} = \frac{4}{3}\cdot\frac{1}{2} = \frac{2}{3}.$$

Deci $\frac{1}{2p} < e^{\frac{2}{3}} < 2$ si $p > \frac{1}{4}$. □

Dimensiunea D a spatiului $H^\perp$ poate fi gasita aplicand algoritmul A de mai multe ori. Daca d este mai mic sau egal decat D, se va gasi o baza cu probabilitate $> 1/4$, altfel ea nu se va gasi deloc. Pentru un interval discret $I = \{k, k+1, \ldots, k+r\}$ fie $M(I)$ mijlocul lui. Fie $B(I)$ partea initiala si $T(I)$ partea finala, cu $T \cup B = I$.

ALGORITM C (determinarea dimensiunii)

Se incepe cu $I = \{0, 1, \ldots, m\}$.

1. Daca I are un singur element, stop.
2. Aplica algoritmul A ca sa decizi daca $D \le M(I)$. Daca da, $I = B(I)$. Altfel $I = T(I)$.
3. Go to 1.

Algoritmul C are nevoie de $log_2 m$ apelari, fiecare aplicare a algoritmului A functioneaza cu probabilitate de $1/4$, deci C functioneaza cu probabilitate de cel putin $1/4^{\log_2 m} = 1/m^2$. Deci C trebuie aplicat $O(m^2)$ ori pentru a determina dimensiunea cu probabilitate constanta.

Observatie: Gasirea ordinului si logaritmul discret sunt probleme inrudite cu aceasta.

14 Metoda Grover de amplificare a probabilitatii

Fie $f : \mathbb{F}_2^n \to \mathbb{F}_2$ o functie necunoscuta, calculata de un black-box. Acestei functii i se asociaza un operator Q_f care are un registru sursa $|x\rangle$ de n qubiti si un qubit tinta $|b\rangle$:

$$Q_f|x\rangle|b\rangle = |x\rangle|b \oplus f(x)\rangle.$$

Q_f este o permutare a bazei spatiului Hilbert de dimensiune 2^{n+1}, deci este unitara. Mai mult:

$$Q_f Q_f|x\rangle|b\rangle = |x\rangle|b \oplus f(x) \oplus f(x)\rangle = |x\rangle|b\rangle,$$

deci Q_f este propria ei inversa.

Un alt mod de a codifica functia booleana f in quantum computing este prin definirea operatorului $V_f : H_{2^n} \to H_{2^n}$, definit prin:

$$V_f|x\rangle = (-1)^{f(x)}|x\rangle, \quad x \in \mathbb{F}_2^n.$$

Din nou $V_f V_f = id$.

Fie $R_n : H_{2^n} \to H_{2^n}$ data de $R_n|\vec{0}\rangle = -|\vec{0}\rangle$ si $R_n|\vec{x}\rangle = |\vec{x}\rangle$ pentru $\vec{x} \neq \vec{0}$. Aceasta este matricea identitate cu $2^n \times 2^n$ elemente, doar ca primul element este inmultit cu -1.

Ne reamintim operatorul Hadamard-Walsh, dat de:

$$H_n|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{\vec{y} \in \mathbb{F}_2^n} (-1)^{\vec{x}\cdot\vec{y}}|y\rangle.$$

Definitie: Operatorul Grover asociat functiei black-box f este definit ca:

$$G_n = -H_n R_n H_n V_f.$$

Vom argumenta in cele ce urmeaza faptul ca G_n produce o amplificare a probabilitatii de gasire a unei valori $\vec{y}$ astfel incat $f(\vec{y}) = 1$. Se calculeaza usor ca:

$$(H_n R_n H_n)_{\vec{x}\vec{y}} = \begin{cases} -\frac{2}{2^n}, & \vec{x} \neq \vec{y}, \\ 1 - \frac{2}{2^n}, & \vec{x} = \vec{y}. \end{cases}$$

Cu alte cuvinte, $H_n R_n H_n = I - 2P$ unde I este identitatea lui H_{2^n} iar P este proiectia pe spatiul de dimensiune 1 generat de:

$$\psi = \frac{1}{\sqrt{2^n}} \sum_{\vec{x} \in \mathbb{F}_2^n} |x\rangle,$$

adica $P = |\psi\rangle\langle\psi|$.

Vom explicita efectul operatorului $-H_n R_n H_n$ pe o superpozitie generala:

$$\sum_{\vec{x} \in \mathbb{F}_2^n} c_{\vec{x}}|x\rangle.$$

Fie media amplitudinilor complexe:

$$A = \frac{1}{2^n} \sum_{\vec{x} \in \mathbb{F}_2^n} c_{\vec{x}}.$$

Se observa ca:

$$\sum_{\vec{x} \in \mathbb{F}_2^n} c_{\vec{x}}|x\rangle = \sum_{\vec{x} \in \mathbb{F}_2^n} (c_{\vec{x}} - A)|x\rangle + \frac{1}{2^n} \sum_{\vec{x} \in \mathbb{F}_2^n} c_{\vec{x}}|x\rangle,$$

si ca aceasta este o descompunere in **vectori ortogonali**. Intr-adevar:

$$\langle A\sum_{\vec{x}}|\vec{x}\rangle \mid \sum_{\vec{y}}(c_{\vec{y}}-A)|\vec{y}\rangle\rangle = \sum_{\vec{x},\vec{y}}A^*(c_{\vec{x}}-A)\langle\vec{x}|\vec{y}\rangle =$$

$$= A^*\sum_{\vec{x}}c_{\vec{x}} - \sum_{\vec{x}}A^*A = A^*2^nA - 2^nA^*A = 0.$$

Asadar:

$$P\sum_{\vec{x}\in\mathbb{F}_2^n}c_{\vec{x}}|x\rangle = A\sum_{\vec{x}\in\mathbb{F}_2^n}|x\rangle,$$

$$-H_nR_nH_n\sum_{\vec{x}\in\mathbb{F}_2^n}c_{\vec{x}}|x\rangle = \sum_{\vec{x}\in\mathbb{F}_2^n}(2A-c_{\vec{x}})|x\rangle.$$

Iata de ce acest operator se numeste **inversion about average**.

Exemplu: Daca $f:\mathbb{F}_2^n\to\mathbb{F}_2$ ia valoarea 1 doar pentru un $\vec{y}$ si zero in rest, dupa aplicarea lui V_f acel $|\vec{y}\rangle$ are coeficient $-1/\sqrt{2^n}$ iar ceilalti vectori binari au $+1/\sqrt{2^n}$. Media este:

$$A = \frac{1}{\sqrt{2^n}}(1-\frac{2}{2^n}) \approx \frac{1}{\sqrt{2^n}}.$$

Inversia de amplitudine $-H_nR_nH_n$ face ca vectorii diferiti de $|\vec{y}\rangle$ sa ramana cu o amplitudine de $2A-1/\sqrt{2^n}\approx 1/\sqrt{2^n}$ in timp ce coeficientul lui $|\vec{y}\rangle$ devine $2A+1/\sqrt{2^n}\approx 3\cdot 1/\sqrt{2^n}$. Asadar probabilitatea de observare a lui $|\vec{y}\rangle$ **creste de** 9 **ori**! □

In cele ce urmeaza ne ocupam de functii booleene generale, care iau valoarea 1 pentru k argumente diferite. Intr-o prima etapa vom considera acest numar k cunoscut.

Fie $T\subset\mathbb{F}_2^n$ multimea acelor $\vec{x}$ astfel incat $f(\vec{x})=1$ si F complementara ei. Daca T are k elemente, F are 2^n-k elemente. Presupunem ca dupa r iteratii ale lui $G_n=-H_nR_nH_nV_f$ se obtine superpozitia:

$$t_r\sum_{\vec{x}\in T}|\vec{x}\rangle + f_r\sum_{\vec{x}\in F}|\vec{x}\rangle.$$

Operatorul V_f produce superpozitia:

$$-t_r\sum_{\vec{x}\in T}|\vec{x}\rangle + f_r\sum_{\vec{x}\in F}|\vec{x}\rangle,$$

care are urmatoarea valoare medie:

$$A = \frac{1}{2^n}(-t_rk + f_r(2^n-k)).$$

Operatorul $-H_nR_nH_n$ aplicat acestei superpozitii, produce superpozitia:

$$t_{r+1}\sum_{\vec{x}\in T}|\vec{x}\rangle + f_{r+1}\sum_{\vec{x}\in F}|\vec{x}\rangle,$$

unde $t_{r+1}=2A-t_r$ si $f_{r+1}=2A-f_r$. Asta se poate scrie in forma urmatoarei recurente lineare:

$$\begin{pmatrix}t_{r+1}\\ f_{r+1}\end{pmatrix} = \begin{pmatrix}1-\frac{2k}{2^n} & 2-\frac{2k}{2^n}\\ -\frac{2k}{2^n} & 1-\frac{2k}{2^n}\end{pmatrix}\begin{pmatrix}t_r\\ f_r\end{pmatrix}$$

cu conditia initiala $t_0=f_0=1/\sqrt{2^n}$. Datorita faptului ca G_n este unitar, toate valorile sirului satisfac relatia:

$$kt_r^2 + (2^n-k)f_r^2 = 1.$$

Asadar se impune o substitutie trigonometrica de forma $t_r = \frac{1}{\sqrt{k}} \sin\theta_r$ si $f_r = \frac{1}{\sqrt{2^n - k}} \cos\theta_r$. Solutia problemei de recurenta este:

$$\begin{aligned} t_r &= \frac{1}{\sqrt{k}} \sin((2r+1)\theta_0), \\ f_r &= \frac{1}{\sqrt{2^n - k}} \cos((2r+1)\theta_0), \end{aligned}$$

unde $\theta_0 \in [0, \pi/2]$ este data de relatia $\sin^2\theta_0 = \frac{k}{2^n}$.

Cautam o valoare a lui r care sa maximizeze probabilitatea de observare a unei solutii. Aceasta s-ar intampla, la modul ideal, daca $(2r+1)\theta_0 = \pi/2$, adica $r = -1/2 + \pi/(4\theta_0)$. Cum $\theta_0^2 \approx \sin^2\theta_0 = k/2^n$, da aproximativ:

$$\left[\frac{\pi}{4}\sqrt{\frac{2^n}{k}}\right]$$

iteratii, probabilitatea de a observa o solutie ar trebui sa fie aproape de 1. Riguros se poate demonstra urmatoarea:

Teorema: *Fie $f : \mathbb{F}_2^n \to \mathbb{F}_2$ astfel incat pentru k valori $\vec{x}$, $f(\vec{x}) = 1$. Presupunem ca $0 < k \leq \frac{3}{4}2^n$ si fie $\theta_0 \in [0, \pi/3)$ astfel incat $\sin^2\theta_0 = k/2^n \leq 3/4$. Dupa $[\pi/(4\theta_0)]$ iteratii ale lui G_n pe superpozitia initiala*

$$\frac{1}{\sqrt{2^n}} \sum_{\vec{x} \in \mathbb{F}_2^n} |\vec{x}\rangle$$

probabilitatea de a observa o solutie a ecuatiei $f(\vec{x}) = 1$ este de cel putin $\frac{1}{4}$.

Demonstratie: Trebuie sa estimam eroarea cand $-1/2 + \pi/(4\theta_0)$ este inlocuit cu $[\pi/(4\theta_0)]$. Evident:

$$[\pi/(4\theta_0)] = -1/2 + \pi/(4\theta_0) + \delta,$$

unde $|\,\delta\,| \leq 1/2$. Deci:

$$2([\pi/(4\theta_0)] + 1)\theta_0 = \pi/2 + 2\delta\theta_0,$$

iar $|\,2\delta\theta\,| \leq \pi/3$. Asadar:

$$\sin^2 2([\pi/(4\theta_0)] + 1)\theta_0 \geq \sin^2(\frac{\pi}{2} - \frac{\pi}{3}) = \frac{1}{4}.$$

□

Grover's Search Algorithm

Input: O functie booleana black-box $f : \mathbb{F}_2^n \to \mathbb{F}_2$ care ia valoarea 1 pentru k argumente $\vec{x}$.
Output: Un $\vec{y} \in \mathbb{F}_2$ cu $f(\vec{y}) = 1$.

1. Daca $k > \frac{3}{4} \cdot 2^n$, alege $\vec{y}$ la intamplare si opreste.
2. Altfel calculeaza $r = [\pi/(4\theta_0)]$ unde $\theta_0 \in [0, \pi/3]$ este dat de $\sin^2\theta_0 = k/2^n$.
3. Folosind transformarea Hadamard H_n se prepara superpozitia initiala:

$$\frac{1}{\sqrt{2^n}} \sum_{\vec{x} \in \mathbb{F}_2^n} |x\rangle.$$

4. Se aplica $G_n = -H_n R_n H_n Q_f$ de r ori.
5. Se observa superpozitia si se citeste un $|\vec{y}\rangle$.

Observatia de la punctul 1 are o probabilitate de succes de cel putin $3/4$. Daca $k = 1$ si n este mare, $r \approx (\pi/4)\sqrt{(2^n)}$. Daca $k = 2^{n-2}$, $\sin^2\theta_0 = 1/4$ si $\theta_0 = \pi/6$. Probabilitatea observarii unei solutii dupa o singura iteratie a lui G_n este $\sin^2(3\theta_0) = 1$. Deci rezultatul va fi observat cu certitudine!

In general insa, nu se cunoaste dinainte valoarea lui k. In cele ce urmeaza vom modifica algoritmul pentru cazul general.

Lemma:

$$\sum_{r=0}^{m-1} \cos((2r+1)\alpha) = \frac{\sin(2m\alpha)}{2\sin\alpha}.$$

Lemma: *Fie $f : \mathbb{F}_2^n \to \mathbb{F}_2$ o functie booleana cu $k \leq (3/4)\cdot 2^n$ solutii $\vec{x}$ pentru ecuatia $f(\vec{x}) = 1$. Fie $\theta_0 \in [0, \pi/3]$ astfel incat $\sin^2\theta_0 = k/2^n \leq 3/4$. Fie m un intreg pozitiv si $r \in [0, m-1]$ ales uniform. Daca G_n se aplica de r ori pe superpozitia initiala*

$$\frac{1}{\sqrt{2^n}} \sum_{\vec{x}\in\mathbb{F}_2^n} |\vec{x}\rangle,$$

probabilitatea de a observa o solutie a ecuatiei $f(\vec{x}) = 1$ este de cel putin:

$$\frac{1}{2} - \frac{\sin(4m\theta_0)}{4m\sin(2\theta_0)}.$$

Demonstratie: Daca r este ales uniform, probabilitatea observarii unei solutii va fi:

$$P \geq \frac{1}{m}\sum_{r=0}^{m-1} \sin^2((2r+1)\theta_0) = \frac{1}{m}\sum_{r=0}^{m-1}(1 - \cos((2r+1)2\theta_0)) = \frac{1}{2} - \frac{\sin(4m\theta_0)}{4m\sin(2\theta_0)}.$$

□

Observam ca daca $m \geq \frac{1}{\sin(2\theta_0)}$ atunci:

$$\sin(4m\theta_0) \leq 1 \leq m\sin(2\theta_0),$$

si deci $P \geq 1/4$.

Quantum Search Algorithm

Input: O functie booleana black-box $f : \mathbb{F}_2^n \to \mathbb{F}_2$.

Output: Un $\vec{y} \in \mathbb{F}_2$ cu $f(\vec{y}) = 1$, daca el exista.

1. Alege $\vec{y}$ la intamplare. Daca $f(\vec{y}) = 1$, opreste.
2. Altfel calculeaza $m = [\sqrt{2^m}] + 1$ si alege r uniform intre 1 si $m - 1$.
3. Folosind transformarea Hadamard H_n se prepara superpozitia initiala:

$$\frac{1}{\sqrt{2^n}} \sum_{\vec{x}\in\mathbb{F}_2^n} |x\rangle.$$

4. Se aplica $G_n = -H_n R_n H_n Q_f$ de r ori.
5. Se observa superpozitia si se citeste un $|\vec{y}\rangle$. Acest $\vec{y}$ este corect cu o probabilitate de cel putin $1/4$.

Asadar orice problema NP-completa se rezolva in timp cuantic $O(\sqrt{2^n}p(n))$, unde $p(n)$ este un polinom care depinde de problema. Acest timp de rezolvare este mai rapid decat orice timp cunoscut clasic.

Part II
Exercitii

15 Matrici stocastice

Exemplu: Dati cu banul folosind o moneda corecta. Se presupune ca de fiecare data cand dam cu banul, starea initiala este rezultatul experimentului anterior. Matricea stocastica este:

$$M = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$$

Se observa ca $M^2 = M$ deci pentru orice $n > 0$, $M^n = M$. Asta inseamna ca nu conteaza de cate ori am dat cu banul. La fiecare noua incercare sansele stau la fel. Nu exista un efect cumulativ.

Exemplu: Dati cu banul folosind o moneda incorecta. Se presupune ca de fiecare data cand dam cu banul, starea initiala este rezultatul experimentului anterior. Matricea stocastica este:

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

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

Se observa din nou ca $M^2 = M$ deci pentru orice $n > 0$, $M^n = M$. Asta inseamna ca nu conteaza de cate ori am dat cu banul. La fiecare noua incercare sansele stau la fel. Nu exista un efect cumulativ.

Exemplu: Un locuitor din Bucuresti si unul din Iasi sunt relativ multumiti de orasele lor. La fiecare moment $t \in \mathbb{N}$ ei ar ramane in orasele lor cu probabilitate $1-\varepsilon$ si s-ar muta in celalalt oras cu probabilitate ε. Matricea stocastica este:

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

Se observa ca pentru $\varepsilon \neq 1/2$, $M^2 \neq M$. Sa se calculeze $\lim_{n\to\infty} M^n$, daca aceasta limita exista.

Vom incepe prin a calcula valorile si vectorii proprii. Ecuatia caracteristica $(X-1+\varepsilon)^2 - \varepsilon^2 = 0$ se scrie $(X-1+2\varepsilon)(X-1) = 0$ cu solutii 1 si $1-2\varepsilon$. Pentru valoarea proprie 1 se obtine vectorul propriu $(1,1)$, iar pentru valoarea proprie $1-2\varepsilon$ se obtine vectorul propriu $(1,-1)$. Cei doi vectori sunt gata ortogonali, deci pentru ortonormalizare trebuie doar impartiti la norma $\sqrt{2}$. Observam asadar ca matricea de schimbare a bazei este matricea Hadamard-Walsh W_2:

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

Fie D matricea diagonala:

$$D = \begin{pmatrix} 1 & 0 \\ 0 & 1-2\varepsilon \end{pmatrix}$$

Cum $W_2^{-1} = W_2$ se obtine ca: $D = W_2 M W_2$, deci $M = W_2 D W_2$ si mai ales $M^n = W_2 D^n W_2$. Cum:

$$\lim_{n\to\infty} D^n = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = L,$$

rezulta ca:

$$\lim_{n\to\infty} M^n = W_2 L W_2 = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$$

Deci la infinit, fiecare va fi schimbat orasul cu probabilitate de $1/2$.

Exemplu: Soarecele si pisica. Cinci incaperi sunt legate prin coridoare in modul urmator:

$$1 \Longleftrightarrow 2 \Longleftrightarrow 3 \Longleftrightarrow 4 \Longleftrightarrow 5.$$

Presupunem ca in primul moment in 1 se afla o pisica si in 5 se afla un soarece. La fecare nou moment $t \rightsquigarrow t+1$ pisica si soarecele se deplaseaza in stanga sau dreapta cu probabilitate egala cu $1/2$. Daca sunt intr-o camera terminala, atunci se vor duce in singura camera accesibila cu probabilitate 1. Tema este intocmirea matricii stocastice pentru acest sistem.

Ideea este ca nu trebuie sa luam in considerare toate combinatiile, ci doar cele la care se poate ajunge. Notam urmatoarele stari:

$$S_1 \ : \ P \Longleftrightarrow 2 \Longleftrightarrow S \Longleftrightarrow 4 \Longleftrightarrow 5.$$
$$S_2 \ : \ P \Longleftrightarrow 2 \Longleftrightarrow 3 \Longleftrightarrow 4 \Longleftrightarrow S.$$
$$S_3 \ : \ 1 \Longleftrightarrow P \Longleftrightarrow 3 \Longleftrightarrow S \Longleftrightarrow 5.$$
$$S_4 \ : \ 1 \Longleftrightarrow 2 \Longleftrightarrow P \Longleftrightarrow 4 \Longleftrightarrow S.$$

De asemeni, fie S_5 starea $(P,S) \in \{(2,2),(3,3),(4,4)\}$, numita stare finala sau *game over*. Cu aceste notatii, matricea stocastica este urmatoarea:

$$\begin{pmatrix} 0 & 0 & 1/2 & 0 & 1/2 \\ 0 & 0 & 1 & 0 & 0 \\ 1/4 & 1/4 & 0 & 1/4 & 1/4 \\ 0 & 0 & 1/2 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

16 Probabilitati si grupuri

Teorema: Fie G un grup finit. Fie P probabilitatea urmatorului eveniment:

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

Daca $P = P(C) > 5/8$ atunci G este abelian.

Demonstratie: Consideram intai centrul grupului G:

$$Z(G) = \{x \in G \,|\, \forall y \ xy = yx\}.$$

Este un subgrup normal in G. Cat poate fi de mare?

Daca $|G : Z(G)| = 1$ atunci $G = Z(G)$ deci G este abelian.

Daca $|G : Z(G)| = 2$ atunci: $\exists u \in G \ \forall x \ x \notin Z(G) \rightarrow \exists y \in Z(G) \ x = uy$. Adica $G = \langle Z(G), u \rangle$ si este abelian. Contradictie.

Daca $|G : Z(G)| = 3$ atunci: $G = Z(G) \cup aZ(G) \cup a^2 Z(G)$ si din nou $G = \langle Z(G), a \rangle$ si este abelian. Contradictie.

Daca $|G : Z(G)| = 4$ atunci: $G/Z(G) \simeq \mathbb{Z}_4$ sau $G/Z(G) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. In primul caz G este abelian. In al doilea caz nu, dupa cum arata exemplul grupului $G = \{\pm 1, \pm i, \pm j, \pm k\}$ unde i, j, k sunt unitatile fundamentale ale cuaternionilor. $Z(G) = \{\pm 1\}$ dar $ij \neq ji$ deci G nu este abelian.

In concluzie, daca G nu este abelian, $|G : Z(G)| \geq 4$.

Pentru un element g care nu este in centru, consideram centralizatorul:

$$C(g) = \{x \in G \,|\, xg = gx\}.$$

Daca $|G : C(g)| = 1$ atunci $g \in Z(G)$. Dar se poate ca $|G : C(g)| = 2$, de exemplu la grupul cuaternionilor $C(i) = \{\pm 1, \pm i\}$.

In concluzie, daca $g \notin Z(G)$ atunci $|G : C(g)| \geq 2$.

Presupunem ca G nu este abelian si alegem $(x, y) \in G \times G$. Cu probabilitate $\leq 1/4$, x comuta cu toate elementele. Cu probabilitate $\geq 3/4$, x comuta cu $\leq 1/2$ din elemente. Asadar:

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

□

17 Cercul complex si sfera reala

Cercul complex este multimea:

$$C = \{(z_1, z_2) \in \mathbb{C}^2 \,|\, z_1^2 + z_2^2 = 1\}.$$

Sfera reala sau sfera qubitilor este multimea:

$$Q = \{(z_1, z_2) \in \mathbb{C}^2 \,|\, |z_1|^2 + |z_2|^2 = 1\}.$$

Ambele sunt incluse in $\mathbb{C}^2$, care se identifica natural cu $\mathbb{R}^4$. C are dimensiune complexa 1 si dimensiune reala 2. Q are dimensiune reala 3 si nu are dimensiune complexa.

C are ecuatia reala $(x_1 + iy_1)^2 + (x_2 + iy_2)^2 = 1$, care este echivalenta cu sistemul:

$$\begin{aligned} 1 + y_1^2 + y_2^2 &= x_1^2 + x_2^2, & (1)\\ x_1y_1 + x_2y_2 &= 0. & (2) \end{aligned}$$

Q este o sfera euclidiana clasica:

$$x_1^2 + y_1^2 + x_2^2 + y_2^2 = 1. \quad (3)$$

Observam ca $(1/2, 1/2, 1/2, 1/2) \in Q \setminus C$ si ca $(i, \sqrt{2}) \in C \setminus Q$. Oare ce multime este $Q \cap C$?

Din ultima ecuatie:

$$x_1^2 + x_2^2 + 1 + y_1^2 + y_2^2 = 2. \quad (4)$$

Din prima ecuatie:

$$\begin{aligned} x_1^2 + x_2^2 &= 1, & (5)\\ y_1^2 + y_2^2 &= 0. & (6) \end{aligned}$$

Deci $(x_1, y_1, x_2, y_2) = (\cos x, 0, \sin x, 0)$. Ecuatia a doua e verificata automat. Deci intersectia ese un cerc real de dimensiune 1.

Ce este C? Daca notam $U = z_1 + iz_2$ si $V = z_1 - iz_2$, ecuatia lui C devine $UV = 1$. Deci C este o hiperbola. Mai exact:

$$\begin{pmatrix} U \\ V \end{pmatrix} = \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$$

Observam ca:

$$W = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$$

este unitara, si ca $WC = \{(U, V) \,|\, UV = \frac{1}{2}\}$.

Ce se poate spune despre transformarile unitare 2×2 ?

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

Adica:

$$\begin{aligned} a\overline{a} + b\overline{b} &= 1, & (7)\\ a\overline{c} + b\overline{d} &= 0, & (8)\\ c\overline{a} + d\overline{b} &= 0, & (9)\\ c\overline{c} + d\overline{d} &= 1. & (10) \end{aligned}$$

Ecuatiile 2 si 3 de mai sus sunt echivalente. Prin urmare cele doua linii sunt in Q, cele doua coloane sunt in Q si $\langle (a,b)|(c,d)\rangle = 0$, adica cele doua linii sunt hermitian ortogonale. Ultima relatie, explicitata in termeni reali, inseamna ca ambele conditii de mai jos sunt adevarate:

$$\begin{aligned} \vec{a}\cdot\vec{c} + \vec{b}\cdot\vec{d} &= 0, & (11)\\ \det\begin{pmatrix} a_1 & c_1 \\ a_2 & c_2 \end{pmatrix} + \det\begin{pmatrix} b_1 & d_1 \\ b_2 & d_2 \end{pmatrix} &= 0. & (12) \end{aligned}$$

18 Seria Fourier finita

Scopul acestui exercitiu este sa exemplifice Seria Fourier Finita a unei multimi de trei elemente si sa ofere o prima aplicatie, si anume rezolvarea ecuatiei de gradul 3.

Fie $z_1, z_2, z_3 \in \mathbb{C}$ si $\omega = \exp(2\pi i/3)$ o radacina primitiva de ordin 3 a unitatii.

Ecuatia $z^3 = 1$ are solutiile 1, ω, ω^2 cu $\omega^2 = \overline{\omega}$ si $1 + \omega + \omega^2 = 0$.

Cautam polinomul $P(z) = \eta_0 + \eta_1 z + \eta_2 z^2$ astfel incat $P(1) = z_0$, $P(\omega) = z_1$, $P(\omega^2) = z_2$.

Seria Fourier finita a sirului z_0, z_1, z_2 se exprima prin relatiile:

$$\begin{aligned} z_0 &= \eta_0 + \eta_1 + \eta_2 & (13)\\ z_1 &= \eta_0 + \eta_1\omega + \eta_2\omega^2 & (14)\\ z_2 &= \eta_0 + \eta_1\omega^2 + \eta_2\omega & (15) \end{aligned}$$

Adica:

$$\begin{pmatrix} z_0 \\ z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \begin{pmatrix} \eta_0 \\ \eta_1 \\ \eta_2 \end{pmatrix} \quad (16)$$

Se observa ca:

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega^2 & \omega \\ 1 & \omega & \omega^2 \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}, \quad (17)$$

deci matricea

$$\Omega = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \quad (18)$$

este unitara intrucat satisface $\Omega\Omega^* = I_3$.

Aplicand matricea inversa sistemului initial, acest sistem se rezolva in modul urmator:

$$\begin{aligned} 3\eta_0 &= z_0 + z_1 + z_2 & (19)\\ 3\eta_1 &= z_0 + z_1\omega^2 + z_2\omega & (20)\\ 3\eta_2 &= z_0 + z_1\omega + z_2\omega^2 & (21) \end{aligned}$$

Se observa ca η_0 este centrul de greutate al triunghiului $\Delta z_0 z_1 z_2$. Putem presupune asadar ca aplicam o translatie cu $-\eta_0$ si avem $\eta_0 = 0$. Atunci triunghiul este de fapt determinat de doua numere complexe η_1 si η_2:

$$\begin{aligned} z_0 &= \eta_1 + \eta_2 && (22)\\ z_1 &= \eta_1\omega + \eta_2\omega^2 && (23)\\ z_2 &= \eta_1\omega^2 + \eta_2\omega && (24) \end{aligned}$$

Din inmultirea celor doua relatii, folosind $\omega^2 + \omega = -1$, obtinem:

$$9\eta_1\eta_2 = z_0^2 + z_1^2 + z_2^2 - z_0z_1 - z_1z_2 - z_0z_2.$$

Pe de alta parte din $z_0 + z_1 + z_2 = 0$ rezulta:

$$z_0^2 + z_1^2 + z_2^2 + 2z_0z_1 + 2z_1z_2 + 2z_0z_2 = 0,$$

Inmultind ultima relatie cu 2 si adunand-o la relatia precedenta se obtine:

$$3\eta_1\eta_2 = -(z_0z_1 + z_1z_2 + z_0z_2).$$

Presupunem ca z_0, z_1, z_2 sunt solutiile ecuatiei cubice:

$$z^3 + pz + q = 0, \quad (25)$$

unde coeficientul lui z^2 este 0 deoarece $z_1 + z_2 + z_3 = 0$.
Din relatiile lui Viete, $p = z_0z_1 + z_1z_2 + z_0z_2$, asadar:

$$3\eta_1\eta_2 = -p. \quad (26)$$

In continuare il vom exprima pe q in functie de η_1 si η_2. Din identitatea:

$$(z-1)(z-\omega)(z-\omega^2) = z^3 - 1, \quad (27)$$

daca inlocuim z cu $-z$, avem identitatea:

$$(z+1)(z+\omega)(z+\omega^2) = z^3 + 1. \quad (28)$$

Daca in aceasta identitate scriem $z = \eta_1/\eta_2$ si omogenizam, apare relatia:

$$(\eta_1 + \eta_2)(\eta_1 + \omega\eta_2)(\eta_1 + \omega^2\eta_2) = \eta_1^3 + \eta_2^3. \quad (29)$$

Daca inmultim a doua paranteza cu ω si a treia paranteza cu ω^2, se obtine:

$$\begin{aligned} (\eta_1 + \eta_2)(\omega\eta_1 + \omega^2\eta_2)(\omega^2\eta_1 + \omega\eta_2) &= \eta_1^3 + \eta_2^3, && (30)\\ z_0z_1z_2 = \eta_1^3 + \eta_2^3 &= -q. && (31) \end{aligned}$$

Daca centralizam informatia din relatiile de mai sus, rezulta sistemul:

$$\begin{aligned} \eta_1^3 + \eta_2^3 &= -q, && (32)\\ \eta_1^3\eta_2^3 &= -\frac{p^3}{27}. && (33) \end{aligned}$$

Deci η_1^3 si η_2^3 sunt solutii ale **rezolventei patratice**:

$$x^2 + qx - \frac{p^3}{27} = 0, \quad (34)$$

asadar

$$\eta_1^3 = -\frac{q}{2} + \sqrt{\Delta}, \tag{35}$$

$$\eta_2^3 = -\frac{q}{2} - \sqrt{\Delta}, \tag{36}$$

unde **discriminantul ecuatiei cubice** este

$$\Delta = \frac{q^2}{4} + \frac{p^3}{27}. \tag{37}$$

Se calculeaza η_1 iar din relatia $\eta_1\eta_2 = -p/3$ se gaseste si η_2.

In continuare se poate face o discutie calitativa a rezultatului. Fie $p, r \in \mathbb{R}$.

1. $\Delta > 0$. Atunci $\eta_1^3 \in \mathbb{R}$, deci η_1 ia o valoare reala si doua valori complexe. In final, z_0 este reala pe cand z_1 si z_2 sunt imaginar conjugate.
2. $\Delta < 0$. Se observa ca $p < 0$ si ca $|\,\eta_1\,| = |\,\eta_2\,|$. Din $\eta_1\eta_2 = -p/3 \in \mathbb{R}$ rezulta $\eta_1 = \overline{\eta}_2$. Din relatiile:

$$z_0 = \eta_1 + \eta_2 \tag{38}$$

$$z_1 = \eta_1\omega + \eta_2\omega^2 \tag{39}$$

$$z_2 = \eta_1\omega^2 + \eta_2\omega \tag{40}$$

   se observa ca $z_0, z_1, z_2 \in \mathbb{R}$.
3. $\Delta = 0$. Atunci $p < 0$. Alegem $\eta_1 = \eta_2$ cu $\eta_1^2 = -p/3$. Rezulta $z_0, z_1, z_2 \in \mathbb{R}$ cu $z_1 = z_2$.

Solutia ecuatiei de gradul 3 a fost descrisa pentru prima oara de catre **Nicolo Tartaglia** in 1535.

Va las ca exercitiu urmatoarea problema de geometrie (Napoleon Bonaparte).

Fie $\Delta\alpha\beta\gamma$ un triunghi oarecare. Se construiesc triunghiurile echilaterale $\Delta\beta\gamma\alpha'$, $\Delta\alpha\gamma\beta'$ si $\Delta\alpha\beta\gamma'$ in exteriorul triunghiului $\Delta\alpha\beta\gamma$. Daca u, v, w sunt centrele noilor triunghiuri, aratati ca Δuvw este echilateral.

19 Aproximatii rationale I

Definitie: Daca $u \in \mathbb{R}$ si $a \in \mathbb{Z}$ este intregul cel mai apropiat, notam cu $||u|| := |u - a|$.

Teorema: *Fie $\theta \in \mathbb{R} \setminus \mathbb{Q}$ si $m \in \mathbb{N}$. Atunci exista $b \in \{0, \ldots, m\}$ astfel incat:*

$$||b\theta|| < \frac{1}{m+1} \tag{41}$$

Demonstratie: Consideram urmatoarele $m + 2$ numere:

$$0, 1, \theta - [\theta], 2\theta - [2\theta], \ldots, m\theta - [m\theta],$$

toate in $[0, 1]$. Exista doua astfel incat:

$$|(k_2\theta - h_2) - (k_1\theta - h_1)| < \frac{1}{m+1} \tag{42}$$

Luam $b = |k_2 - k_1|$ si $a = h_2 - h_1$. □

Observatie: $\frac{1}{m+1} < \frac{1}{b}$, deci $||b\theta|| < b^{-1}$. *Aceasta se intampla pentru o infinitate de b.* Intr-adevar, daca ar fi adevarat doar pentru $b_1, \ldots, b_r$, fie m astfel incat $1/m < ||b_j\theta||$ pentru toti j. Atunci exista b cu:

$$||b\theta|| < \frac{1}{m+1} < \frac{1}{m} < ||b_j\theta||$$

pentru toti j, deci $||b\theta|| < b^{-1}$ desi $b \neq b_1, \ldots, b_r$. Asadar am demonstrat urmatoarea teorema:

Teorema: *Daca $\theta \in \mathbb{R} \setminus \mathbb{Q}$ exista o infinitate de numere rationale a/b astfel incat:*

$$\left|\theta - \frac{a}{b}\right| \quad < \quad \frac{1}{b^2} \tag{43}$$

Aici puterea lui b nu se poate imbunatati, dar coeficientul lui da.

Definitie: Sirul lui Farey este sirul ordonat:

$$F_n = \{x \in \mathbb{Q} \,|\, x = \frac{a}{b} \text{ ireductibila cu } 0 < b \leq n\}.$$

De exemplu:

$$F_7 : \cdots - \frac{1}{6}, -\frac{1}{7}, \frac{0}{1}, \frac{1}{7}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{2}{7}, \frac{1}{3}, \frac{2}{5}, \frac{3}{7}, \cdots$$

Teorema: *Daca $\frac{a}{b} < \frac{c}{d}$ sunt fractii consecutive in sirul Farey, atunci $bc - ad = 1$.*

Demonstratie: Inductie dupa n. Pentru $n = 1$, $\frac{a}{1} < \frac{a+1}{1}$ si $(a+1) - a = 1$. OK.

Trecerea de la n la $n+1$. Fie $\frac{a}{b} < \frac{c}{d}$ fractii consecutive in F_n. Atunci $b + d \geq n + 1$ pentru ca altfel $(a+c)/(b+d) \in F_n$ si

$$\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d},$$

ceea ce contravine ipotezei ca fractiile erau consecutive.

Daca in F_{n+1} aceste fractii raman consecutive, stim deja ca $bc - ad = 1$. Daca apare o fractie intre ele, ea il va avea pe $n+1$ la numitor. Fie $k/(n+1)$ o astfel de fractie. Atunci:

$$\frac{1}{bd} = \frac{c}{d} - \frac{a}{b} = \frac{c}{d} - \frac{k}{n+1} + \frac{k}{n+1} - \frac{a}{b} = \frac{c(n+1) - dk}{d(n+1)} + \frac{bk - a(n+1)}{b(n+1)}$$

Fie:

$$u \quad = \quad c(n+1) - dk \geq 1, \tag{44}$$

$$v \quad = \quad bk - a(n+1) \geq 1. \tag{45}$$

Vom arata ca $u = 1$ si $v = 1$. Daca macar unul este > 1 atunci:

$$\frac{1}{bd} > \frac{1}{d(n+1)} + \frac{1}{b(n+1)} \leftrightarrow n + 1 > b + d \leftrightarrow \perp.$$

Deci:

$$\frac{c}{d} - \frac{k}{n+1} = \frac{1}{d(n+1)} \quad , \quad \frac{k}{n+1} - \frac{a}{b} = \frac{1}{d(n+1)},$$

adica $c(n+1) - kd = 1$ si $kb - (n+1)a = 1$. Pe de alta parte intre ele nu pot aparea mai multe fractii deoarece un $h/(n+1)$ ar avea proprietatea ca:

$$\frac{h}{n+1} - \frac{a}{b} = \frac{1}{b(n+1)} = \frac{k}{n+1} - \frac{a}{b},$$

deci $h = k$. □

Teorema: *Fie $\theta \in \mathbb{R} \setminus \mathbb{Q}$ si $r \in \mathbb{N} \setminus \{0\}$. Atunci pentru n suficient de mare, fractiile consecutive a/b si c/d din F_n care au proprietatea ca:*

$$\frac{a}{b} < \theta < \frac{c}{d}$$

au numitorii $b > r$ si $d > r$.

Demonstratie: Fie $m_1, m_2, \ldots, m_r$ intregii cei mai apropiati de $\theta, 2\theta, \ldots, r\theta$. Alegem n suficient de mare astfel incat:

$$\frac{1}{n} < \left|\theta - \frac{m_j}{j}\right|$$

pentru toti j. Fie q orice intreg astfel incat pentru toti $j = 1, 2, \ldots, r$,

$$|j\theta - m_j| \leq |j\theta - q| \leftrightarrow \left|\theta - \frac{m_j}{j}\right| \leq \left|\theta - \frac{q}{j}\right|$$

Aceasta implica:

$$\frac{1}{n} < \left|\theta - \frac{q}{j}\right|$$

Diferentele dintre fractiile consecutive din F_n sunt $\leq 1/n$. Deci daca a/b si c/d sunt fractii consecutive din F_n cu proprietatea ca

$$\frac{a}{b} < \theta < \frac{c}{d},$$

atunci

$$\left|\theta - \frac{a}{b}\right| < \left|\frac{c}{d} - \frac{a}{b}\right| \leq \frac{1}{n} \quad , \quad \left|\theta - \frac{c}{d}\right| < \left|\frac{c}{d} - \frac{a}{b}\right| \leq \frac{1}{n}.$$

Deci este necesar ca $b > r$ si $c > r$.

20 Aproximatii rationale II

Scopul acestei serii de exercitii este demonstrarea Teoremei lui Hurwitz din 1891.

Lema: *NU exista $x, y \in \mathbb{N} \setminus \{0\}$ care satisfac simultan urmatoarele inegalitati:*

$$\frac{1}{xy} \geq \frac{1}{\sqrt{5}}\left(\frac{1}{x^2} + \frac{1}{y^2}\right) \tag{46}$$

$$\frac{1}{x(x+y)} \geq \frac{1}{\sqrt{5}}\left(\frac{1}{x^2} + \frac{1}{(x+y)^2}\right) \tag{47}$$

Demonstratie: Inmultim prima relatie cu $\sqrt{5}x^2y^2$ si a doua relatie cu $\sqrt{5}x^2(x+y)^2$, ne da:

$$0 \geq x^2 + y^2 - \sqrt{5}x^2y^2 \tag{48}$$

$$0 \geq (2 - \sqrt{5})(x^2 + xy) + y^2 \tag{49}$$

Adunam aceste relatii, si restrangem:

$$0 \geq [(\sqrt{5} - 1)x - 2y]^2 \tag{50}$$

Acest lucru este imposibil pentru $x/y \in \mathbb{Q}$. □

Teorema lui Hurwitz: *Fie $\theta \in \mathbb{R} \setminus \mathbb{Q}$. Atunci exista o infinitate de numere rationale h/k astfel incat:*

$$\left|\theta - \frac{h}{k}\right| < \frac{1}{\sqrt{5}k^2} \tag{51}$$

Numarul $\sqrt{5}$ este cel mai bun posibil si nu se poate inlocui cu unul mai mare.

Demonstratie: Fie a/b si c/d fractii consecutive din sirul lui Farey F_n astfel incat:

$$\frac{a}{b} < \theta < \frac{c}{d}$$

Cazul I:

Are loc inegalitatea:

$$\frac{a}{b} < \frac{a+c}{b+d} < \theta < \frac{c}{d}.$$

Aratam ca inegalitatile urmatoare nu pot avea loc simultan:

$$\theta - \frac{a}{b} \geq \frac{1}{\sqrt{5}b^2} \tag{52}$$

$$\theta - \frac{a+c}{b+d} \geq \frac{1}{\sqrt{5}(b+d)^2} \tag{53}$$

$$\frac{c}{d} - \theta \geq \frac{1}{\sqrt{5}d^2} \tag{54}$$

Adunam prima si ultima relatie:

$$\frac{c}{d} - \frac{a}{b} \geq \frac{1}{\sqrt{5}}\Big(\frac{1}{b^2} + \frac{1}{d^2}\Big).$$

Dar cum

$$\frac{1}{bd} = \frac{c}{d} - \frac{a}{b},$$

rezulta

$$\frac{1}{bd} \geq \frac{1}{\sqrt{5}}\Big(\frac{1}{b^2} + \frac{1}{d^2}\Big). \tag{55}$$

Adunam celelalte doua relatii:

$$\frac{c}{d} - \frac{a+c}{b+d} \geq \frac{1}{\sqrt{5}}\Big(\frac{1}{b^2} + \frac{1}{(b+d)^2}\Big).$$

Dar cum

$$\frac{1}{b(b+d)} = \frac{c}{d} - \frac{a+c}{b+d},$$

rezulta

$$\frac{1}{b(b+d)} \geq \frac{1}{\sqrt{5}}\Big(\frac{1}{b^2} + \frac{1}{(b+d)^2}\Big). \tag{56}$$

Contradictie cu Lema.

Cazul II:

Are loc inegalitatea:

$$\frac{a}{b} < \theta < \frac{a+c}{b+d} < \frac{c}{d}.$$

Rezolvarea este analoga Cazului I.

Deci inegalitatea are loc pentru unul din elementele $h/k \in \{a/b, c/d, (a+c)/(b+d)\}$. Deoarece n a fost ales arbitrar, gasim o infinitate de astfel de numere rationale.

Acum aratam ca $\sqrt{5}$ este cea mai buna constanta. Fie *numerele de aur*:

$$\theta_0 = \frac{1+\sqrt{5}}{2} \quad , \quad \theta_1 = \frac{1-\sqrt{5}}{2}.$$

Cum $(x-\theta_0)(x-\theta_1) = x^2 - x - 1$, are loc:

$$\Big|\frac{h}{k} - \theta_0\Big|\Big|\frac{h}{k} - \theta_1\Big| = \Big|\Big(\frac{h}{k}\Big)^2 - \frac{h}{k} - 1\Big| \neq 0$$

Dar $\theta_1 = \theta_0 - \sqrt{5}$.

$$\Big|\frac{h}{k} - \theta_0\Big|\Big|\frac{h}{k} - \theta_0 + \sqrt{5}\Big| = \frac{|h^2 - hk - k^2|}{k^2} \geq \frac{1}{k^2}.$$

$$\frac{1}{k^2} \leq \Big|\frac{h}{k} - \theta_0\Big|\Big(\Big|\frac{h}{k} - \theta_0\Big| + \sqrt{5}\Big).$$

Fie acum un $\beta > 0$ cu proprietatea ca exista o infinitate de h_j/k_j astfel incat:

$$\Big|\theta - \frac{h_j}{k_j}\Big| \quad < \quad \frac{1}{\beta k_j^2} \tag{57}$$

Deci daca inlocuim modulul din ultima relatie in relatia anterioara, obtinem:

$$\frac{1}{k_j^2} < \frac{1}{\beta k_j^2}\Big(\frac{1}{\beta k_j^2} + \sqrt{5}\Big).$$

$$\beta \leq \frac{1}{\beta k_j^2} + \sqrt{5}.$$

Asta se intampla pentru toti j. Putem alege un subsir cu $k_j \to \infty$. Deci $\beta \leq \sqrt{5}$. □

21 Teorema lui Jesse Douglas

Iata o alta aplicatie a serieii Fourier discrete. Scopul ei este urmatoarea teoreme de Jesse Douglas.

Teorema: *Fie* $\Pi = (z_0, z_1, \ldots, z_4) \subset \mathbb{R}^3$ *un pentagon stramb inchis in spatiul euclidian 3-dimensional. Notam cu:*

$$z'_j = \frac{z_{j+2} + z_{j-2}}{2}$$

mijlocul laturii opuse lui z_j. *Pe dreapta care uneste* z_j *cu* z'_j *se construiesc punctele* f_1^j *si* f_2^j *astfel incat:*

$$f_1^j - z_j = \frac{1}{\sqrt{5}}(z'_j - z_j) \quad , \quad f_2^j - z'_j = -\frac{1}{\sqrt{5}}(z'_j - z_j).$$

Atunci punctele f_1^j *definesc un pentagon plan afin regulat* Π^1 *iar punctele* f_2^j *definesc un poligon plan stelat afin regulat* Π^2.

Observatie: Un poligon afin regulat este imaginea unui poligon regulat printr-o transformare afina. Configuratia de puncte si segmente de dreapta definita in ipoteza se poate realiza in practica. Constructia rezultata are un aspect de structura abstracta si sugereaza aparitia ordinii din haos. Ca informaticieni, puteti programa un applet optic 3D in care utilizatorul sa poata eventual modifica coordonate sau le poate misca interactiv. Pentagoanele Π, Π^1 si Π^2 ar trebui reprezentate cu culori diferite.

Dimensiune 2: Pentru inceput, presupunem ca pentagonul Π se afla intr-un plan, deci $\Pi \subset \mathbb{C}$. Fie $\omega_j = \exp(\frac{2\pi ij}{5})$ radacinile de ordin 5 ale unitatii. Fie η_j coeficientii Fourier discreti ai sirului z_i. Asadar:

$$z_j = \eta_0 + \eta_1\omega_j + \eta_2\omega_j^2 + \eta_3\omega_j^3 + \eta_4\omega_j^4, \quad j = 0, 1, 2, 3, 4.$$

Notand $\eta_3 = \eta_{-2}$ si $\eta_4 = \eta_{-1}$ rescriem aceste relatii ca:

$$z_j = \eta_0 + (\eta_1\omega_j + \eta_{-1}\omega_j^{-1}) + (\eta_2\omega_j^2 + \eta_{-2}\omega_j^{-2}).$$

Notam:

$$f_1^j = \eta_1\omega_j + \eta_{-1}\omega_j^{-1} \quad , \quad f_2^j = \eta_2\omega_j^2 + \eta_{-2}\omega_j^{-2}.$$

Deocamdata aceste puncte **nu** sunt cele din enunt. Acest lucru va fi aratat mai tarziu. Deocamdata observam ca:

$$z_j = \eta_0 + f_1^j + f_2^j.$$

Ca si la exercitiul cu ecuatia de gradul 3, putem presupune fara a restrange generalitatea ca $\eta_0 = 0$ deci ca:

$$z_j = f_1^j + f_2^j.$$

Fie acum Π^1 si Π^2 pentagoanele definite de aceste puncte f^j.

Aratam ca Π^1 este afin regulat si ca Π^2 este stelat afin regulat. Fie $f_1^j = x_j + iy_j$, $\eta_1 = a + bi$ si $\eta_{-1} = c + di$. Atunci:

$$\begin{aligned} x_j &= (a+c)\cos\frac{2\pi j}{5} + (-b+d)\sin\frac{2\pi j}{5}, \\ y_j &= (b+d)\cos\frac{2\pi j}{5} + (a-c)\sin\frac{2\pi j}{5}. \end{aligned}$$

$$\begin{pmatrix} x_j \\ y_j \end{pmatrix} = \begin{pmatrix} a+c & -b+d \\ b+d & a-c \end{pmatrix} \begin{pmatrix} \cos\frac{2\pi j}{5} \\ \sin\frac{2\pi j}{5} \end{pmatrix}$$

Deci Π^1 este poligon afin regulat. Demonstratia pentru Π^2 este asemanatoare. □

Acum vom demonstra ca pentagoanele Π^1 si Π^2 sunt exact cele din enunt. Fie $\omega = \omega_1$. Atunci:

$$\begin{aligned} z_{j+2} &= (\eta_1\omega_j\omega^2 + \eta_{-1}\omega_j^{-1}\omega^{-2}) + (\eta_2\omega_j^2\omega^{-1} + \eta_{-2}\omega_j^{-2}\omega), \\ z_{j-2} &= (\eta_1\omega_j\omega^{-2} + \eta_{-1}\omega_j^{-1}\omega^2) + (\eta_2\omega_j^2\omega + \eta_{-2}\omega_j^{-2}\omega^{-1}). \end{aligned}$$

$$z'_j = \frac{z_{j+2} + z_{j-2}}{2} = \frac{1}{2}(\omega^2 + \omega^{-2})f_1^j + \frac{1}{2}(\omega + \omega^{-1})f_2^j.$$

Cum $\cos\frac{4\pi}{5} = -\cos\pi 5$ se obtine sistemul:

$$\begin{aligned} z_j &= f_1^j + f_2^j, \\ z'_j &= -f_1^j\cos\frac{\pi}{5} + f_j^2\cos 2\pi 5. \end{aligned}$$

Se aplica faptul ca $\cos\frac{\pi}{5} = \frac{1}{4}(1+\sqrt{5})$ si $\cos\frac{2\pi}{5} = \frac{1}{4}(-1+\sqrt{5})$. Se rezolva sistemul si se obtin relatiile din enunt pentru f_1^j si f_2^j. □

Dimensiune 3: Fie Π_{xy} si Π_{xz} proiectiile pentagonului Π pe planele Oxy si Oxz.

Lema: *Daca proiectiile plane Π_{xy} si Π_{xz} sunt pentagoane afin regulate, atunci Π este un pentagon plan afin regulat.*

Demonstratie: Presupunem ca Π_{xy} are coordonatele:

$$\begin{aligned} x_j &= a\cos\frac{2\pi j}{5} + b\sin\frac{2\pi j}{5}, \\ y_j &= c\cos\frac{2\pi j}{5} + d\sin\frac{2\pi j}{5}, \end{aligned}$$

iar Π_{xz} are coordonatele:

$$\begin{aligned} x'_j &= a'\cos\frac{2\pi j}{5} + b'\sin\frac{2\pi j}{5}, \\ z_j &= e\cos\frac{2\pi j}{5} + f\sin\frac{2\pi j}{5}. \end{aligned}$$

Din $x_j = x'_j$ pentru toti j rezulta $a = a'$ si $b = b'$. Rezulta ca Π este afin regulat. De asemeni rezulta ca Π este inclus in planul generat de vectorii (a, c, e) si (b, d, f). □

Ca ultim exercitiu, aratati ca Π, Π^1 si Π^2 au acelasi centru de greutate.

22 Operatori autoadjuncti

Scopul acestei serii de exercitii este familiarizarea cu operatorii autoadjuncti complecsi.

Fie H un spatiu vectorial finit dimensional complex si $T : H \to H$ un operator linear.

Definitie: Norma operatorului se defineste:

$$||T|| \quad = \quad \sup_{||x||=1} ||T(x)||. \tag{58}$$

Definitie: Un vector $x \in H$ se numeste vector propriu iar un scalar $\lambda \in \mathbb{C}$ se numeste valoare proprie corespunzatoare lui x daca si numai daca are loc relatia:

$$Tx \quad = \quad \lambda x. \tag{59}$$

Definitie: Operatorul $T^* : H \to H$ se numeste adjunctul lui T daca si numai daca:

$$\forall\, x, y \in H \qquad \langle x|Ty\rangle \quad = \quad \langle T^*x|y\rangle. \tag{60}$$

Aratati ca $T^* = \ ^t(\overline{T})$, adica conjugatul complex al matricii transpuse.

Definitie: T se numeste autoadjunct daca si numai daca $T^* = T$. T se numeste unitar daca si numai daca $T^* = T^{-1}$.

Observatie: Un operator autoadjunct are valori proprii reale.

$$\lambda^*\langle x|x\rangle = \langle \lambda x|x\rangle = \langle Tx|x\rangle = \langle x|Tx\rangle = \lambda\langle x|x\rangle,$$

unde $x \neq 0$ este vector propriu. Deci $\lambda = \lambda^*$. □

Observatie: Fie T autoadjunct, $x, x' \in H$ vectori proprii, $\lambda, \lambda' \in \mathbb{C}$ valori proprii corespunzatoare, cu $\lambda \neq \lambda'$. Atunci $x \perp x'$.

$$\lambda'\langle x'|x\rangle = \langle Tx'|x\rangle = \langle x'|Tx\rangle = \lambda\langle x'|x\rangle.$$

Cum $\lambda' \neq \lambda$ rezulta ca $\langle x'|x\rangle = 0$. □

Definitie: Pentru $x, y \in H$ definim operatorul $|x\rangle\langle y| : H \to H$ in modul urmator:

$$|x\rangle\langle y|z \quad = \quad \langle y|z\rangle x. \tag{61}$$

Daca $||x|| = 1$ atunci $|x\rangle\langle x|$ este proiectia ortogonala pe spatiul vectorial generat de x.

Teorema: Daca $T : H \to H$ este un operator autoadjunct, atunci exista o baza ortonormala a lui H formata din vectorii proprii ai lui T.

Demonstratie: Pentru $\lambda \in \mathbb{C}$ valoare proprie, $H_\lambda = \{v \,|\, Tv = \lambda v\}$ este subspatiu vectorial. Atunci $TH_\lambda \subseteq H_\lambda$ si $TH_\lambda^\perp \subseteq H_\lambda^\perp$, deoarece daca $x \in H_\lambda$ iar $y \in H_\lambda^\perp$ atunci:

$$\langle x|Ty\rangle = \langle Tx|y\rangle = \lambda^*\langle x|y\rangle = 0.$$

Deci studiem restrictiile $T \,|\, H_\lambda$ si $T \,|\, H_\lambda^\perp$ si aplicam pe fiecare ipoteza de inductie. □

Definitie: **Reprezentarea spectrala a operatorilor autoadjuncti**. Fie $T : H \to H$ operator autoadjunct, $x_1, x_2, \ldots, x_n$ baza ortonormala formata din vectori proprii, si $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{R}$ valori proprii corespunzatoare. Atunci reprezentarea spectrala este:

$$T = \lambda_1|x_1\rangle\langle x_1| + \lambda_2|x_2\rangle\langle x_2| + \cdots + \lambda_n|x_n\rangle\langle x_n|. \tag{62}$$

Observatie: **In mecanica cuantica, operatorii autoadjuncti corespund actiunilor de masurare.** Conform filozofiei cuantice, orice masurare intervine in sistem si il influenteaza. In tot cazul, masuratorile distrug superpozitiile cuantice, cauzand asa zisa decoherenta.

Exemplu: Operatorul cuantic de negatie:

$$M_\neg = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{63}$$

Observam ca $M_\neg^* = M_\neg$ deci este autoadjunct. Dupa cum stim, acest operator este si unitar.
Valorile proprii sunt solutia ecuatiei:

$$\det \begin{pmatrix} x & -1 \\ -1 & x \end{pmatrix} = 0,$$

adica $x = \pm 1$. Cautam vectorii propri:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \ \rightarrow \ a = b \ \rightarrow \ v_{+1} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = - \begin{pmatrix} a \\ b \end{pmatrix} \ \rightarrow \ a = -b \ \rightarrow \ v_{-1} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Prin urmare retinem proiectiile:

$$|v_{+1}\rangle\langle v_{+1}| = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \end{pmatrix} = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix},$$

$$|v_{-1}\rangle\langle v_{-1}| = \frac{1}{2} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \begin{pmatrix} 1 & -1 \end{pmatrix} = \begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix}.$$

Ele duc la urmatoarea reprezentare spectrala:

$$M_\neg = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = 1 \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} - 1 \begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix}. \tag{64}$$

Cu ajutorul reprezentarii spectrale se pot calcula alti operatori derivati din acesta. De exemplu:

$$\sqrt{M_\neg} = \sqrt{1} \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix} + \sqrt{-1} \begin{pmatrix} 1/2 & -1/2 \\ -1/2 & 1/2 \end{pmatrix}. \tag{65}$$

Cum $\sqrt{1} = \pm 1$ si $\sqrt{-1} = \pm i$, sunt patru operatori care joaca rolul de radacina patrata a negatiei. □

23 Operatori unitari

In aceste exercitii se realizeaza legatura dintre cele doua feluri de operatori.

Ne reamintim ca pentru $x \in H$ matricea $|x\rangle\langle x|$ este un operator autoadjunct de rang 1. De asemeni, daca $x \perp y$ atunci:

$$(|x\rangle\langle x|)(|y\rangle\langle y|) = |x\rangle(\langle x||y\rangle)\langle y| = 0.$$

Definitie: Fie $T : H \rightarrow H$ un operator autoadjunct si $\{x_1, \ldots, x_n\}$ o baza ortogonala in raport cu care T are reprezentarea spectrala:

$$T = \lambda_1 |x_1\rangle\langle x_1| + \cdots + \lambda_n |x_n\rangle\langle x_n|.$$

Definim:

$$e^{iT} = e^{i\lambda_1}|x_1\rangle\langle x_1| + \cdots + e^{i\lambda_n}|x_n\rangle\langle x_n|. \quad (66)$$

Observatie: e^{iT} este unitar:

$$(e^{iT})^* = e^{-i\lambda_1}|x_1\rangle\langle x_1| + \cdots + e^{-i\lambda_n}|x_n\rangle\langle x_n| = (e^{iT})^{-1}.$$

In realitate, fiecare operator unitar este exponentiala unui operator autoadjunct.

Lema: Fie $A, B : H \to H$ autoadjuncti, unde A are valori proprii λ_i iar B are valori proprii μ_j. Atunci $AB = BA$ daca si numai daca A si B admit aceeasi baza ortogonala de vectori proprii, caz in care:

$$AB = \lambda_1\mu_1|x_1\rangle\langle x_1| + \cdots + \lambda_n\mu_n|x_n\rangle\langle x_n|.$$

□

Fie $U : H \to H$ operator unitar. Intai observam ca daca $\lambda \in \mathbb{C}$ este valoare proprie, atunci $|\lambda| = 1$. Daca $x \neq 0$ este vector propriu si $Ux = \lambda x$, atunci intr-adevar:

$$\langle x|x\rangle = \langle x|U^*Ux\rangle = \langle Ux|Ux\rangle = \langle \lambda x|\lambda x\rangle = \lambda^*\lambda\langle x|x\rangle = |\lambda|^2\langle x|x\rangle.$$

Fie $U = A + iB$ unde $A = \frac{1}{2}(U + U^*)$ si $B = \frac{1}{2i}(U - U^*)$. Observam ca A si B sunt autoadjuncti si comuta unul cu celalalt. Intr-adevar:

$$A^* = \frac{1}{2}(U^* + U) = A,$$

$$B^* = (-\frac{1}{2i})(U^* - U) = B,$$

$$AB = \frac{1}{4i}(U + U^{-1})(U - U^{-1}) = \frac{1}{4i}(U^2 - U^{-2}),$$

$$BA = \frac{1}{4i}(U - U^{-1})(U + U^{-1}) = \frac{1}{4i}(U^2 - U^{-2}).$$

Deci exista o baza ortonormala $\{x_1, \ldots, x_n\}$ comuna, formata din vectori proprii. Deci:

$$A = \lambda_1|x_1\rangle\langle x_1| + \cdots + \lambda_n|x_n\rangle\langle x_n|, \quad (67)$$

$$B = \mu_1|x_1\rangle\langle x_1| + \cdots + \mu_n|x_n\rangle\langle x_n|. \quad (68)$$

Cum valorile proprii ale lui U au norma 1, rezulta ca $|\lambda_i| \leq 1$ si $|\mu_i| \leq 1$, acestea fiind proiectii. Cum A si B sunt atoadjuncti, $\lambda_i, \mu_i \in \mathbb{R}$. Adica $\lambda_i, \mu_i \in [-1, 1]$. Cum $U = A + iB$, avem:

$$U = (\lambda_1 + i\mu_1)|x_1\rangle\langle x_1| + \cdots + (\lambda_n + i\mu_n)|x_n\rangle\langle x_n|.$$

Dar cum $|\lambda_i + i\mu_i| = 1$, exista un $\theta_i \in \mathbb{R}$ astfel incat $\lambda_i = \cos\theta_i$ si $\mu_i = \sin\theta_i$. Cu alte cuvinte $\lambda_j + i\mu_j = e^{i\theta_j}$ si:

$$U = e^{iH}, \text{unde} \quad (69)$$

$$H = \theta_1|x_1\rangle\langle x_1| + \cdots + \theta_n|x_n\rangle\langle x_n|. \quad (70)$$

Se observa ca H este autoadjunct. Operatorul H este Hamiltonianul care il genereaza pe U.

Exemplu: Operatorul Hadamard-Walsh

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

este atat unitara cat si autoadjuncta. Polinomul caracteristic este X^2-1 cu solutii ± 1. Vectorii proprii sunt:

$$v_1 = \frac{1}{\sqrt{4+2\sqrt{2}}}(1+\sqrt{2},1), \tag{71}$$

$$v_{-1} = \frac{1}{\sqrt{4-2\sqrt{2}}}(1-\sqrt{2},1). \tag{72}$$

$$|v_1\rangle\langle v_1| = \frac{1}{4}\begin{pmatrix} 2+\sqrt{2} & \sqrt{2} \\ \sqrt{2} & 2-\sqrt{2}\end{pmatrix} \quad , \quad |v_{-1}\rangle\langle v_{-1}| = \frac{1}{4}\begin{pmatrix} 2-\sqrt{2} & -\sqrt{2} \\ -\sqrt{2} & 2+\sqrt{2}\end{pmatrix}$$

Deci reprezentarea spectrala a operatorului autoadjunct W_2 este:

$$W_2 = 1\cdot|v_1\rangle\langle v_1| + (-1)\cdot|v_{-1}\rangle\langle v_{-1}|.$$

Dar acum observam ca $1 = e^{i0}$ si $-1 = e^{i\pi}$, asadar $W_2 = e^{iT}$ este reprezentarea spectrala a lui W_2 ca operator unitar, unde:

$$T = \pi|v_{-1}\rangle\langle v_{-1}|.$$

In final,

$$W_2 = e^{i\cdot\frac{1}{4}\left(\begin{smallmatrix} 2-\sqrt{2} & -\sqrt{2} \\ -\sqrt{2} & 2+\sqrt{2}\end{smallmatrix}\right)}.$$

□

Exemplu: Rotatia plana este matricea:

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta\end{pmatrix}.$$

Cum $R_\theta^* R_\theta = I_2$, matricea este unitara.

Polinomul caracteristic este $X^2 - 2\cos\theta X + 1$ cu solutii $e^{\pm i\theta}$.

Vectorii propri sunt:

$$x_+ = \frac{1}{\sqrt{2}}(i,1) \quad , \quad x_- = \frac{1}{\sqrt{2}}(-i,1).$$

Proiectiile pe spatiile generate de vectorii proprii sunt:

$$|x_+\rangle\langle x_+| = \frac{1}{2}\begin{pmatrix} 1 & i \\ -i & 1\end{pmatrix} \quad , \quad |x_-\rangle\langle x_-| = \frac{1}{2}\begin{pmatrix} 1 & -i \\ i & 1\end{pmatrix}.$$

$$R_\theta = \frac{1}{2}e^{i\theta}\begin{pmatrix} 1 & i \\ -i & 1\end{pmatrix} + \frac{1}{2}e^{-i\theta}\begin{pmatrix} 1 & -i \\ i & 1\end{pmatrix}.$$

Este imediat ca $R_\theta = e^{iH_\theta}$ unde

$$H_\theta = \frac{1}{2}\theta\begin{pmatrix} 1 & i \\ -i & 1\end{pmatrix} + \frac{1}{2} - \theta\begin{pmatrix} 1 & -i \\ i & 1\end{pmatrix} = \begin{pmatrix} 0 & i\theta \\ -i\theta & 0\end{pmatrix}.$$

Deci in final:

$$R_\theta = e^{\left(\begin{smallmatrix} 0 & -\theta \\ \theta & 0\end{smallmatrix}\right)}.$$

Acest fapt ne mai permite usor verificarea unei ipoteze. Daca generalizam seria exponentiala la matrici, avem definitia:

$$e^A = I + A + \frac{1}{2!}A^2 + \frac{1}{3!}A^3 + \dots$$

Asa se poate verifica prin calcul direct ca:

$$e^{\left(\begin{smallmatrix} 0 & -\theta \\ \theta & 0\end{smallmatrix}\right)} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta\end{pmatrix}.$$

□

24 Relatia lui Heisenberg

Fie $\langle x, y\rangle = \overline{x}_1 y_1 + \cdots + \overline{x}_n y_n$. $\langle x, x\rangle = \| x \|^2$ *este real si ne-negativ.* $A : \mathbb{C}^n \to \mathbb{C}^n$ *liniar satisface* $\langle x, Ay\rangle = \langle A^* x, y\rangle$, *unde* $A^* = (\overline{A})^T$. *A se numeste autoadjunct daca verifica identitatea* $A^* = A$. *Asta implica* $\langle x, Ay\rangle = \langle Ax, y\rangle$.

1. Aratati ca daca A este autoadjunct, atunci pentru orice $x \in \mathbb{C}^n$ are loc $\langle x, Ax\rangle \in \mathbb{R}$.

Pentru A autoadjunct si $x \in \mathbb{C}^n$ *stare cuantica,* $E_x(A) = \langle x, Ax\rangle$ *este expectatia observabilei A. Notam* $\langle x, Ax\rangle := \mu_A \in \mathbb{R}$.

2. Aratati ca daca A este autoadjunct si $r \in \mathbb{R}$, $A - rI$ si $(A - rI)^2$ sunt autoadjuncti.

Definim varianta observabilei A in starea x ca fiind expectatia lui $(A - \mu_A I)^2$, *asadar:*

$\mathrm{Var}_x(A) = E_x((A - \mu_A I)^2) = \langle x, (A - \mu_A I)^2 x\rangle$.

3. Aratati ca $\mathrm{Var}_x(A) = \| (A - \mu_A I)x \|^2$.

4. Demonstrati inegalitatea Cauchy-Schwartz complexa $\| u \|^2 \| v \|^2 \geq |\langle u, v\rangle|^2$. Indicatie: calculati $\| u - \lambda v \|^2$ pentru $\lambda = \langle u, v\rangle / \| v \|^2$. Se dezvolta in λ si se inlocuieste la sfarsit.

Rezulta ca:

$$\mathrm{Var}_x(A)\mathrm{Var}_x(B) \geq |\langle (A - \mu_A I)x, (B - \mu_B I)x\rangle|^2.$$

Pentru $A, B : \mathbb{C}^n \to \mathbb{C}^n$ *fie comutatorul* $[A, B] := AB - BA$.

5. Aratati ca daca A si B sunt autoadjuncti, atunci $[A, B]^* = -[A, B]$. Aratati ca $C := -i[A, B]$ este autoadjunct.

Notam $A_1 := A - \mu_A I$, $B_1 = B - \mu_B I$.

6. Aratati ca daca A si B sunt autoadjuncti, atunci $[A_1, B_1] = [A, B]$ si ca $A_1 B_1 + B_1 A_1$ este autoadjunct.

7. Folositi faptul ca $A_1 B_1 = \frac{1}{2}(A_1 B_1 + B_1 A_1) + \frac{1}{2}(A_1 B_1 - B_1 A_1)$ si aratati ca:

$$|\langle A_1 x, B_1 x\rangle|^2 = \frac{1}{4}|\langle x, (A_1 B_1 + B_1 A_1)x\rangle + i\langle x, Cx\rangle|^2.$$

8. Cum valorile $\langle x, (A_1 B_1 + B_1 A_1)x\rangle$ si $\langle x, Cx\rangle$ sunt numere reale, concludeti ca:

$$\mathrm{Var}_x(A)\mathrm{Var}_x(B) \geq \frac{1}{4}\langle x, Cx\rangle^2 = \frac{1}{4}|\langle x, [A, B]x\rangle|^2,$$

Tocmai ati demonstrat varianta hermitiana a relatiei de incertitudine a lui Heisenberg:

$$\mathrm{Var}_x(A)\mathrm{Var}_x(B) \geq \frac{1}{4}|\langle x, [A, B]x\rangle|^2.$$

Exemple de operatori autoadjuncti A si B care nu comuta, sunt pozitia si momentul, ceea ce implica o relatie inrudita cu cea enuntata initial de Werner Heisenberg.