Ismétlés

HÁLÓZATI RENDSZEREK
ÉS SZOLGÁLTATÁSOK
TANSZÉK

© Mark Parisi, Permission required for use.

Keresés rendezetlen adatbázisban

"Man - a being in search of meaning."

Plato

Dr. Imre Sándor, Dr. Bacsári László

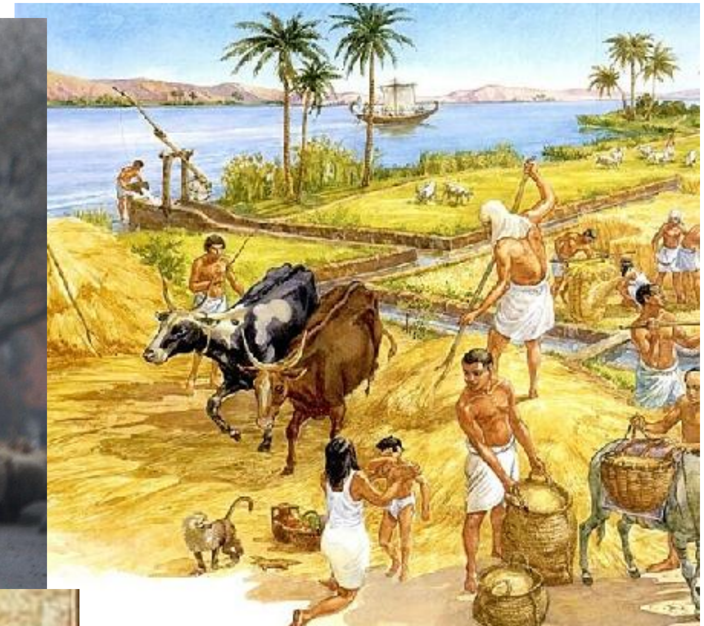
BME Hálózati Rendszerek és Szolgáltatások Tanszék
imre@hit.bme.hu

MŰEGYETEM 1782

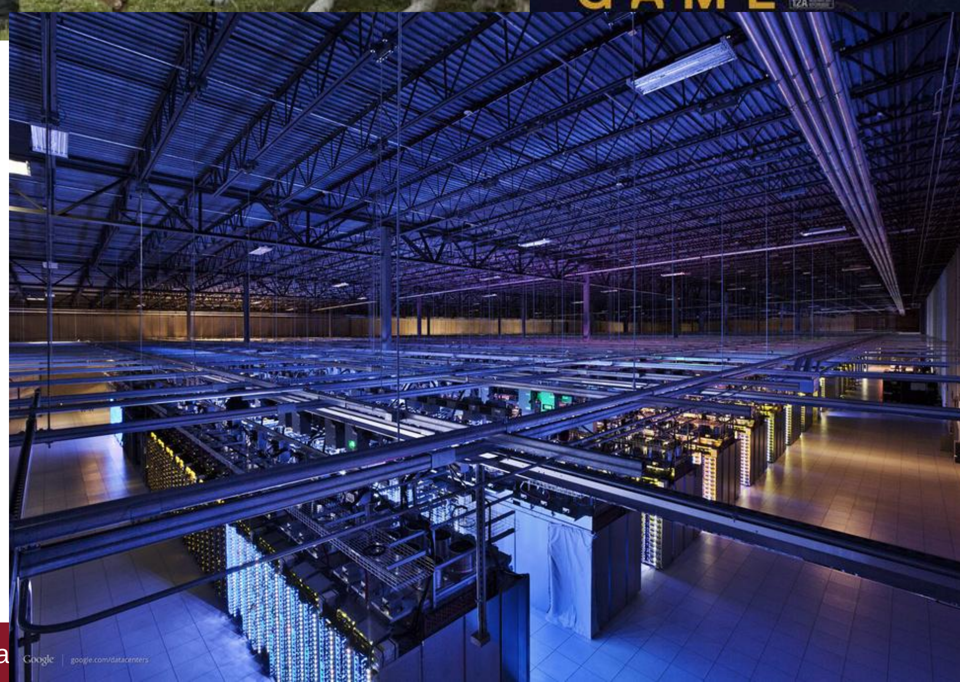
- Másodpercenként hatalmas mennyiségű adatot gyűjtünk az interneten keresztül különféle rendszerekből.
- Csak akkor tudjuk őket hasznosítani, ha elég gyorsan tudjuk feldolgozni őket.

ADATBÁZISKERESÉS TÖRTÉNETE V1

ADATBÁZISKERESÉS TÖRTÉNETE V2

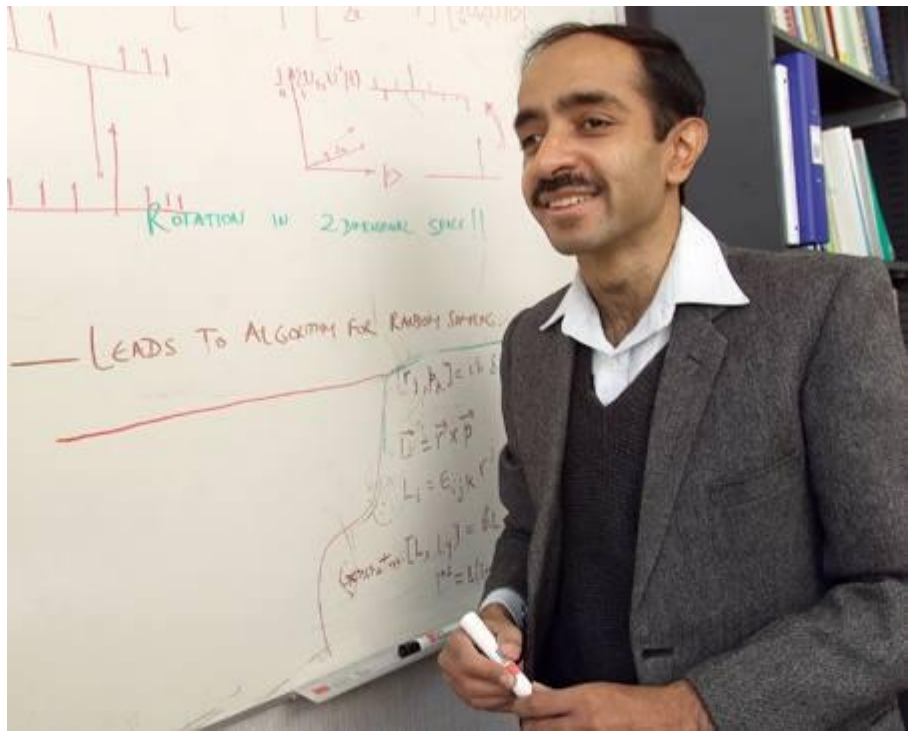


ADATBÁZISKERESÉS TÖRTÉNETE V3



ADATBÁZISKERESÉS TÖRTÉNETE V3

ADATBÁZISKERESÉS TÖRTÉNETE V4
A GROVER-ALGORITMUS



A FELADAT

- Legyen egy rendezetlen DB adatbázisunk, mely *N* elemből áll.
- Az elemeket az *x*-változóval indexeljük.
- Az adatbázisban a keresett elem *M*-szer fordul elő.
- A legjobb klasszikus megoldás *N*-*M*-1 lekérdezéssel találja meg biztosan az egyik keresett elemet.
- A találat azt jelenti, hogy meg tudjuk mondani a keresett elemre mutató indexértéket.

elemek

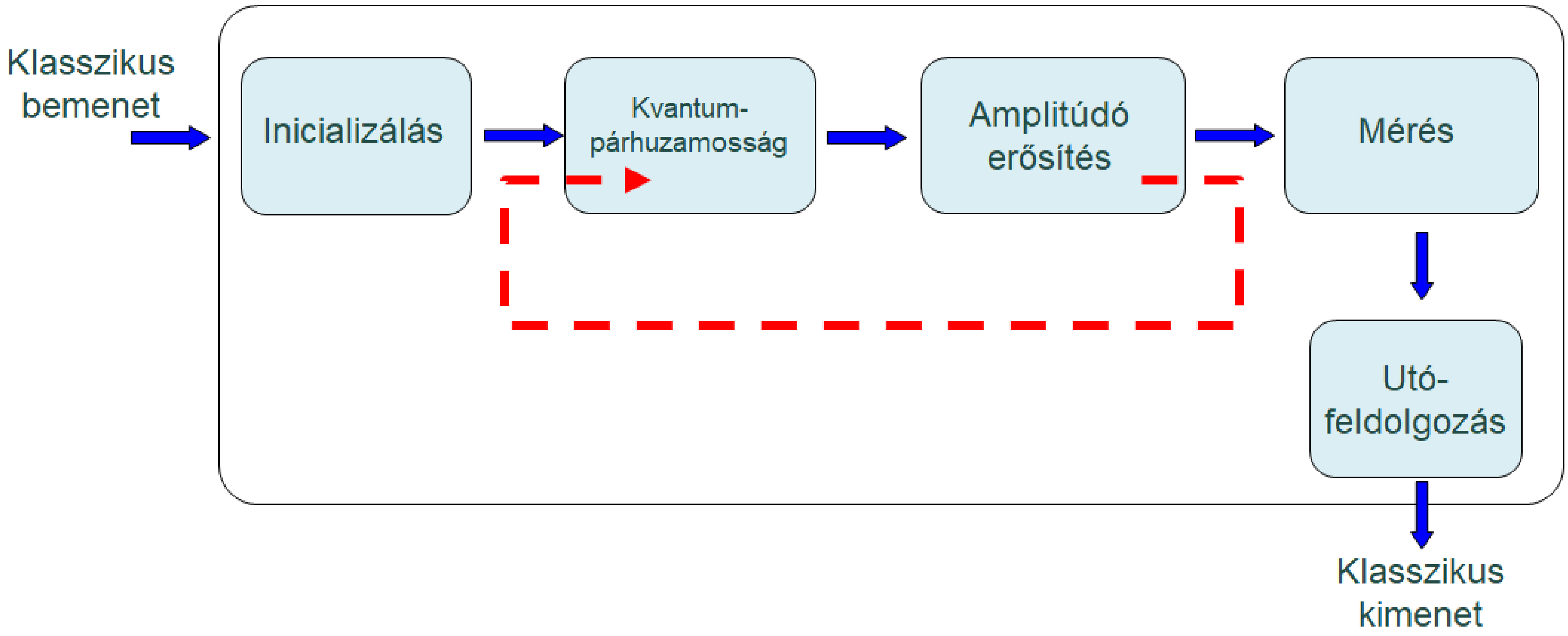
Data base: greengrocer's	
0	apple
1	banana
2	tomato
3	carrot
4	potato
5	raspberry
6	onion
7	celery
8	grape
9	peach
10	melon

x_0

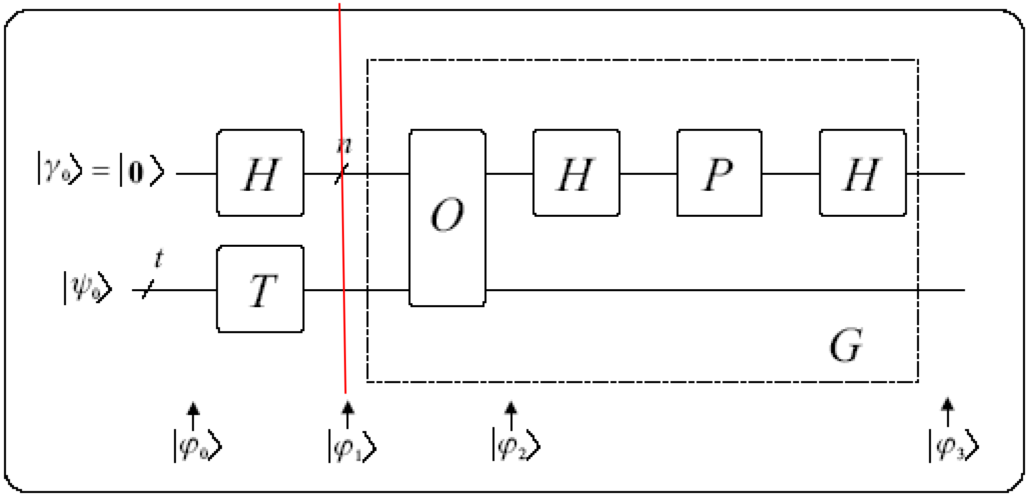
Keresett elem

indexek

KVANTUMALGORITMUSOK TERVEZÉSI RECEPTJE

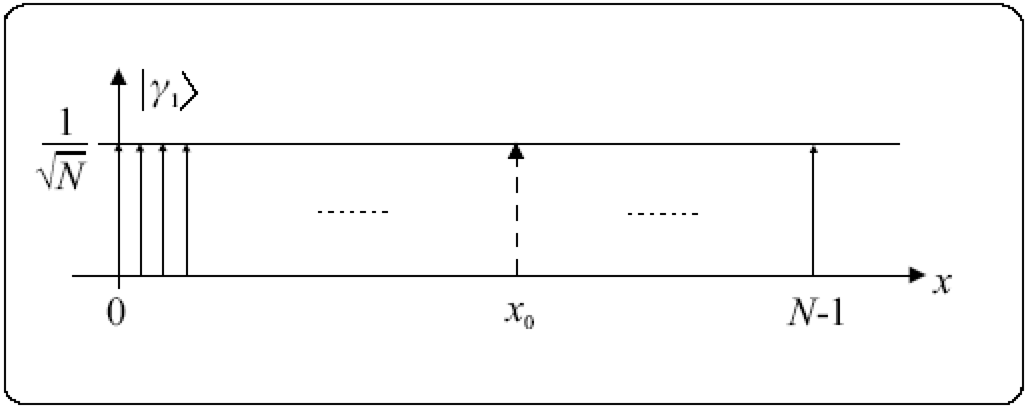


A GROVER-OPERÁTOR MŰKÖDÉSE

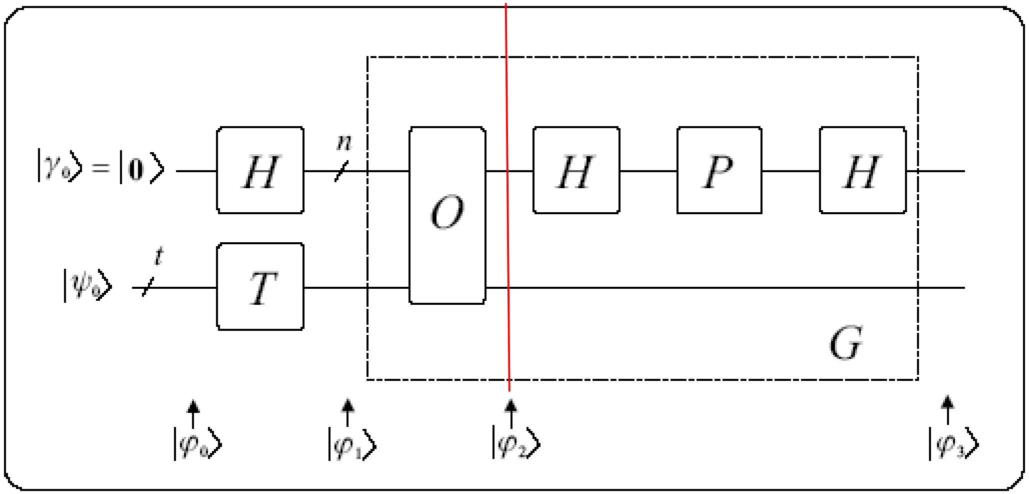


$$|\gamma_1\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

$$|\varphi_1\rangle = \left(H^{\otimes n} \otimes T^{\otimes t}\right)\left(|\gamma_0\rangle \otimes |\psi_0\rangle\right) = \frac{1}{\sqrt{N}} \sum_{x=0} |x\rangle \otimes T|\psi_0\rangle$$



A GROVER-OPERÁTOR MŰKÖDÉSE – ORÁKULUM



$$O : |x\rangle|y\rangle \rightarrow (-1)^{f(x)}|x\rangle|y\rangle$$

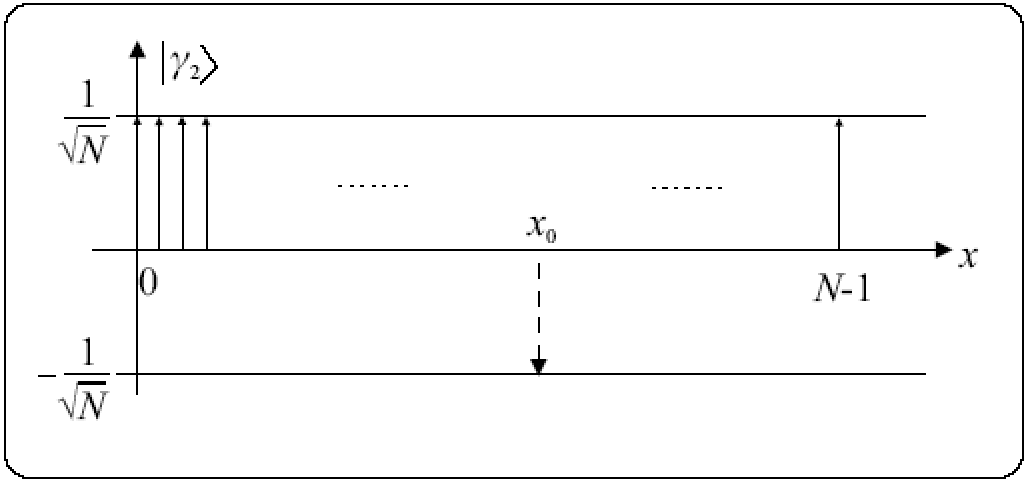
$$f(x) = \begin{cases} 1 & \text{if } x = x_0 \\ 0 & \text{otherwise.} \end{cases}$$

$$|\varphi_2\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}(-1)^{f(x)}|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$|\psi_0\rangle = |1\rangle$

$T = H$

$$O = I - 2|x_0\rangle\langle x_0|.$$

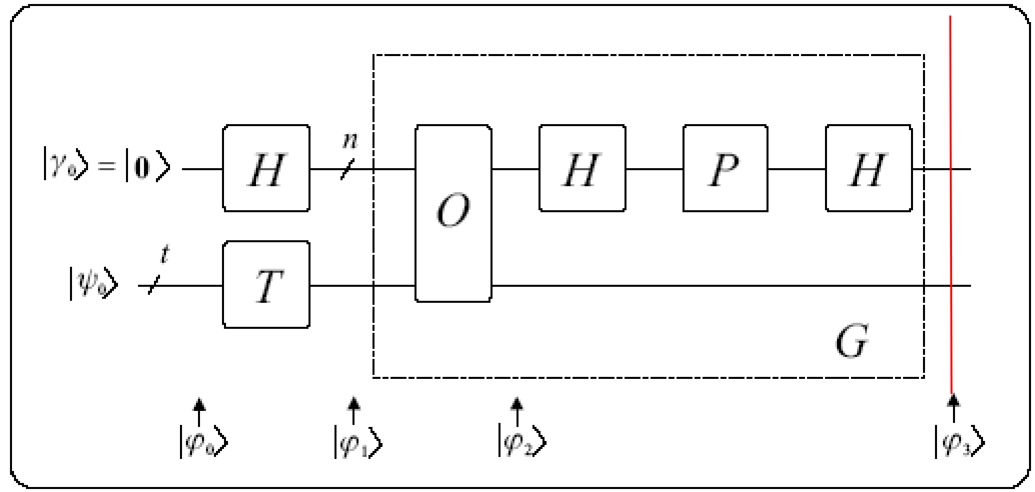


$$\mathbf{O} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

A GROVER-OPERATOR MŰKÖDÉSE - ÁTLAGRA VALÓ TÜKRÖZÉS

$$\overline{a} = \frac{1}{N}\sum_{x=0}^{N-1}\gamma_{2x}$$

$$\gamma_{3x} = 2\overline{a} - \gamma_{2x}$$



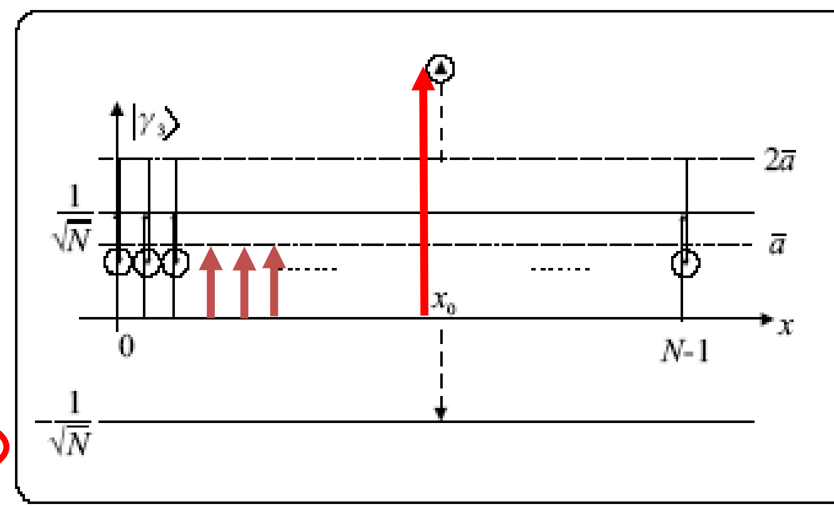
$$|\gamma_3\rangle = \sum_{x=0}^{N-1}(2\overline{a} - \gamma_{2x})|x\rangle = 2\sum_{x=0}^{N-1}\overline{a}|x\rangle - \sum_{x=0}^{N-1}\gamma_{2x}|x\rangle$$

$$\boxed{G = HPHO}$$

$$\langle\gamma_1|\gamma_2\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}\gamma_{2x} = \sqrt{N}\overline{a}$$

$$|\gamma_3\rangle = 2|\gamma_1\rangle\langle\gamma_1||\gamma_2\rangle - |\gamma_2\rangle$$

$$U_\gamma = 2|\gamma_1\rangle\langle\gamma_1| - I = H(2|\mathbf{0}\rangle\langle\mathbf{0}| - I)H$$



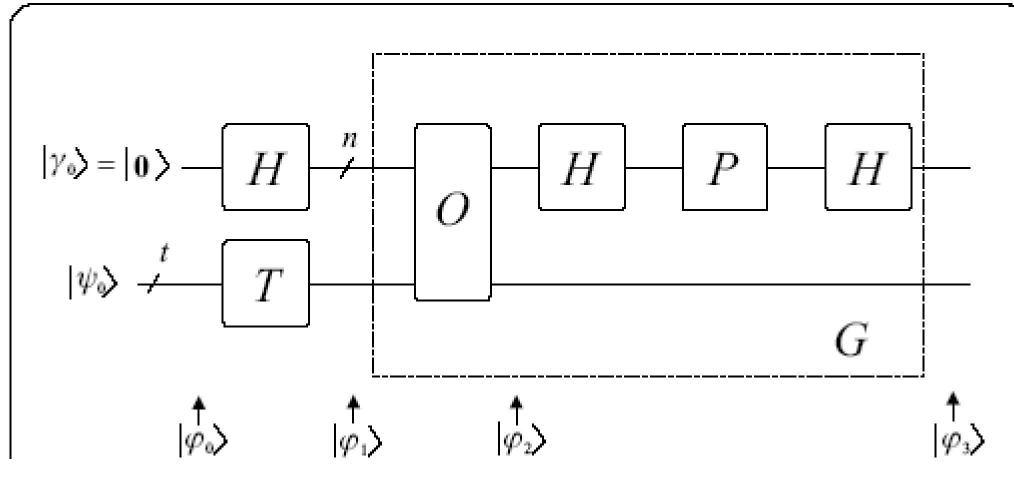
GEOMETRIAI INTERPRETÁCIÓ

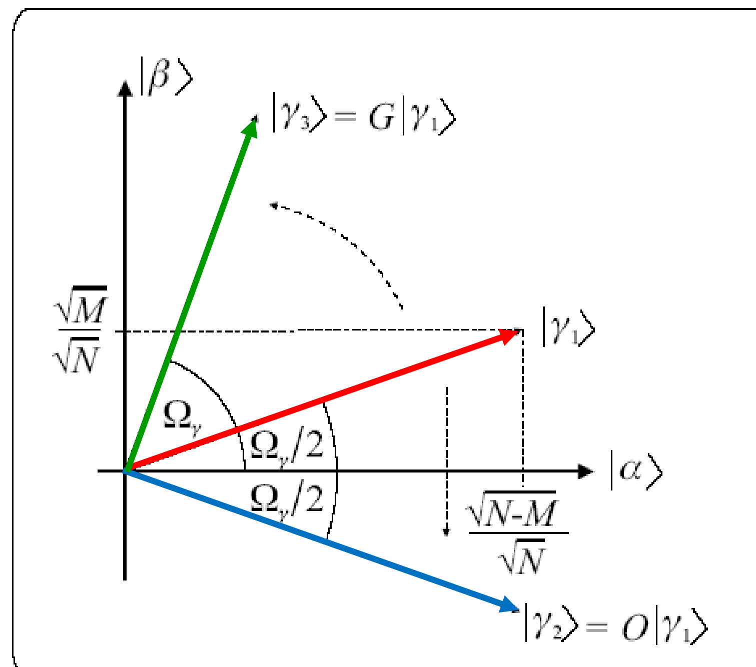
$$|\alpha\rangle \triangleq \frac{1}{\sqrt{N-M}} \sum_{x \in \overline{S}} |x\rangle,$$

$$|\beta\rangle \triangleq \frac{1}{\sqrt{M}} \sum_{x \in S} |x\rangle,$$

$$|\gamma_1\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \overline{S}} |x\rangle + \frac{1}{\sqrt{N}} \sum_{x \in S} |x\rangle,$$

$$= \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle.$$





AZ ITERÁCIÓK SZÁMÁNAK MEGHATÁROZÁSA

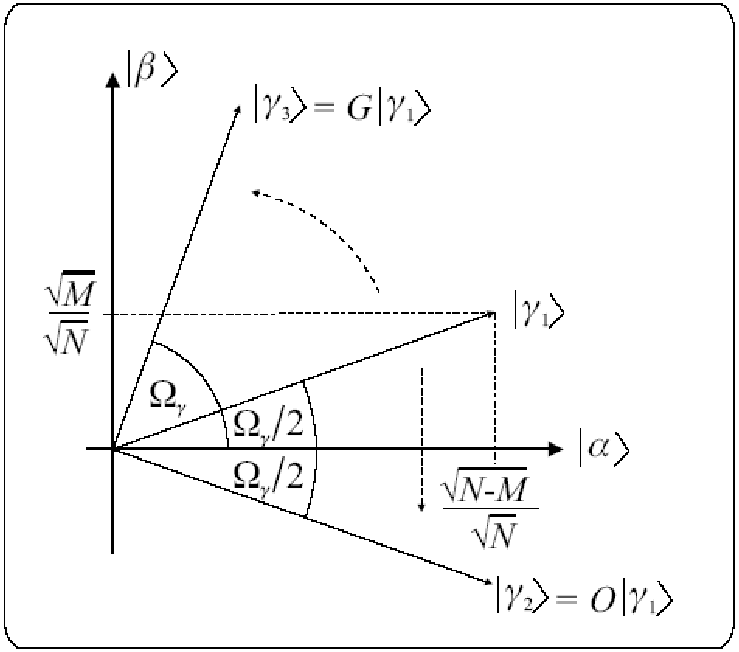
$$G^l|\gamma_1\rangle \quad = \quad \cos\left(l\Omega_\gamma + \frac{\Omega_\gamma}{2}\right)|\alpha\rangle + \sin\left(l\Omega_\gamma + \frac{\Omega_\gamma}{2}\right)|\beta\rangle$$

$$\langle\alpha|G^l|\gamma_1\rangle = \cos\left(\frac{2l+1}{2}\Omega_\gamma\right) = 0 \qquad\qquad l_{opt_i} = \frac{\frac{\pi}{2} + i\pi - \frac{\Omega_\gamma}{2}}{\Omega_\gamma}$$

$$L_{opt_0} = \lfloor l_{opt_0} \rceil = \left\lfloor \frac{\frac{\pi}{2} - \frac{\Omega_\gamma}{2}}{\Omega_\gamma} \right\rceil$$

$$\frac{\Omega_\gamma}{2} \simeq \sin\left(\frac{\Omega_\gamma}{2}\right) = \sqrt{\frac{M}{N}}$$

$$L_{opt_0} = \left\lfloor \frac{\pi}{4}\sqrt{\frac{N}{M}} - 1 \right\rceil \simeq \frac{\pi}{4}\sqrt{\frac{N}{M}}.$$

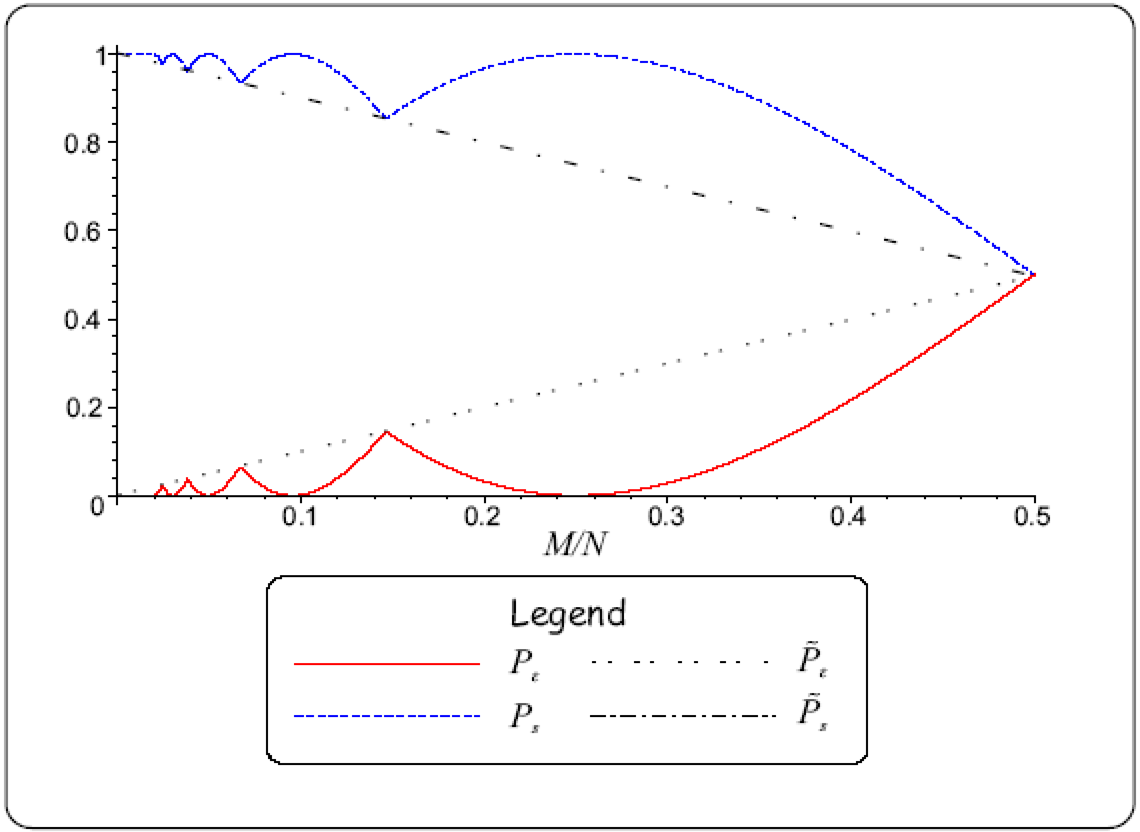


HIBAANALÍZIS

$$P_\varepsilon = |\langle\alpha|G^{L_{opt_0}}|\gamma_1\rangle|^2 = \cos^2\left(\frac{(2L_{opt_0}+1)\,\Omega_\gamma}{2}\right)$$

$$P_\varepsilon \le \sin^2\left(\frac{\Omega_\gamma}{2}\right)$$

$$P_\varepsilon \le \frac{M}{N} = \tilde{P}_\varepsilon$$



KÉRDÉSEK

- Mi történik ha $M=N/2$?
- Mit csináljunk ha $M>N/2$?
- Lehet egyetlen lépéssel megtalálni a keresett elemet?
- Hogyan csökkentsük a tévesztés valószínűségét?
  - 1. ötlet
  - 2. ötlet

- Szimulációs szemléltetés!

Kvantum számlálás és szélsőérték keresés, általánosított Grover-algoritmus

Dr. Imre Sándor , Dr. Bacsárdi László

BME Hálózati Rendszerek és Szolgáltatások Tanszék

imre@hit.bme.hu

Budapest,
2025. 12. 01.

KVANTUMOS SZÁMLÁLÁS–SPECIÁLIS FÁZISBECSLÉS

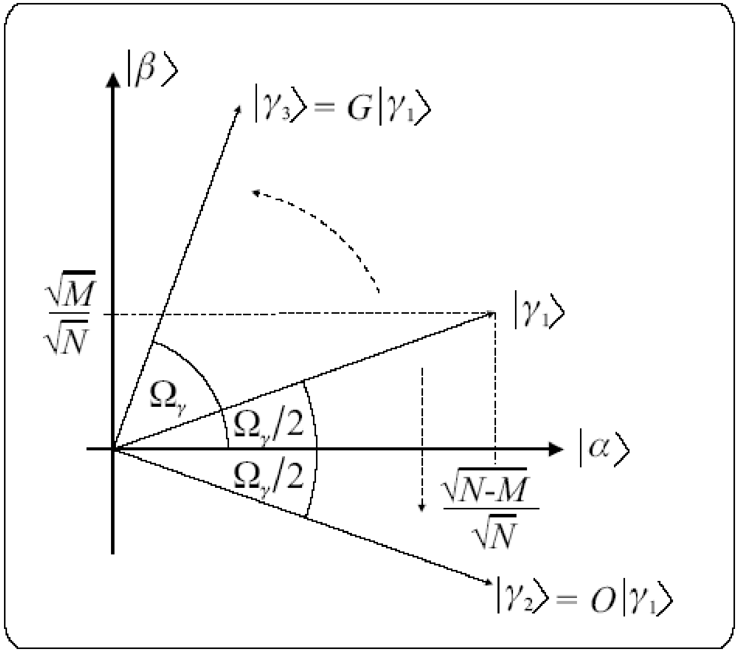
- *M* kiszámítása visszavezethető a Grover-operátoron végrehajtott fázisbecslésre.

$$\mathbf{G} = \begin{bmatrix} \cos(\Omega_\gamma) & -\sin(\Omega_\gamma) \\ \sin(\Omega_\gamma) & \cos(\Omega_\gamma) \end{bmatrix}$$

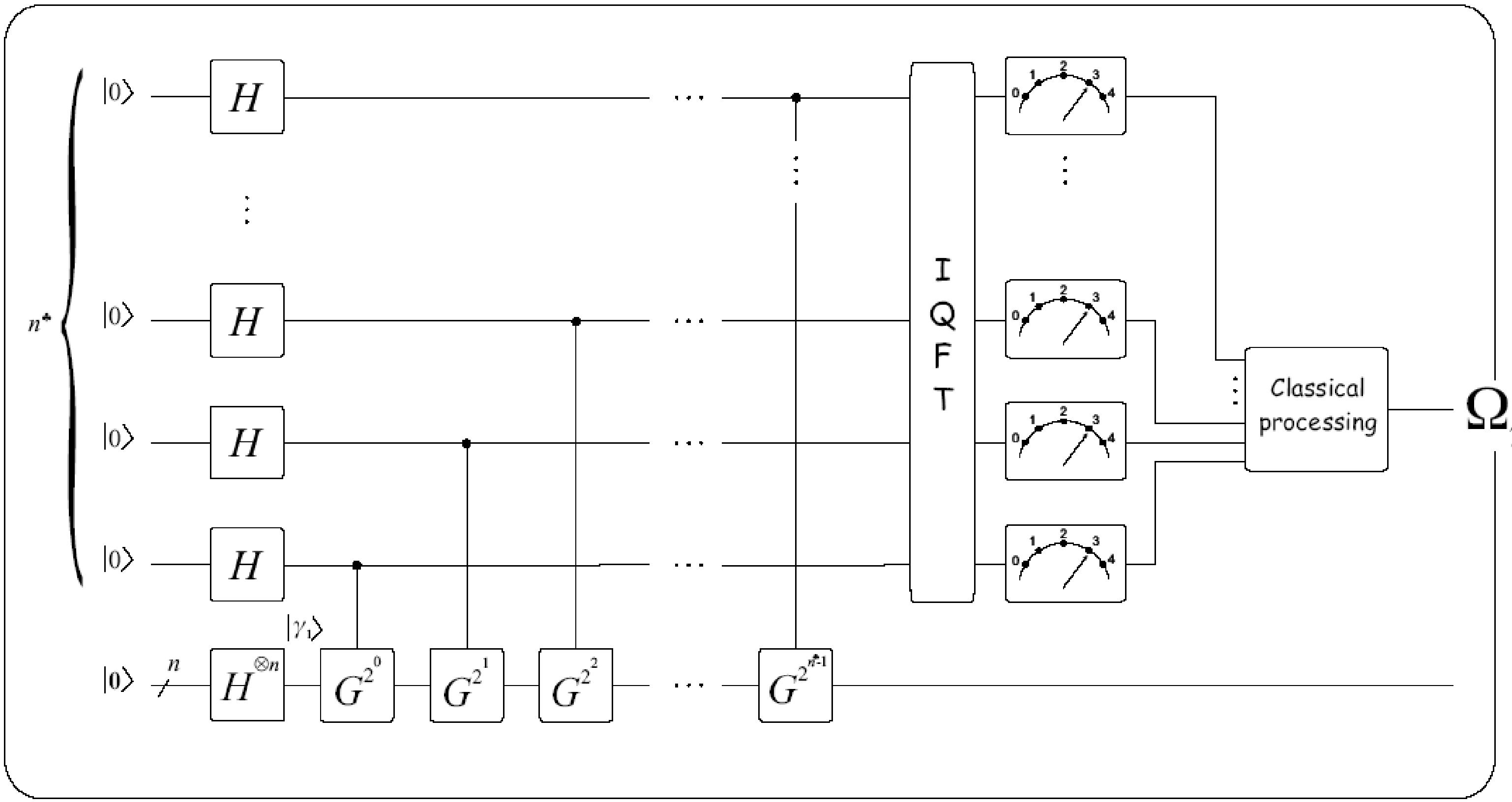
$$|g_1\rangle = \frac{e^{j\xi}}{\sqrt{2}}\begin{bmatrix} j \\ 1 \end{bmatrix}, |g_2\rangle = \frac{e^{j\xi}}{\sqrt{2}}\begin{bmatrix} -j \\ 1 \end{bmatrix}, \xi \in \mathbb{R}$$

$$e^{\pm j\Omega_\gamma}$$

$$\mathbf{U}_{N\times N} = \sum_{u=0}^{N-1} \omega_u |u\rangle\langle u|$$



KVANTUMOS SZÁMLÁLÁS– SPECIÁLIS FÁZISBECSLÉS



$$n^{\clubsuit} = c - 1 + \left\lceil \mathrm{ld}(2\pi) + \mathrm{ld}\left(3 + \frac{1}{\breve{P}_{\varepsilon P}}\right) \right\rceil$$

RSA FELTÖRÉSE GROVER ALGORITMUSSAL

Table 9.1 Code-breaking methods and related complexity

Method	$n = 128$	$n = 128$	$n = 1024$	$n = 1024$	1s barrier
BF	$1.8 \cdot 10^{7}$ s	0.58 year	$1.3 \cdot 10^{142}$ s	$4 \cdot 10^{134}$ year	80 bit
BC	$6 \cdot 10^{-4}$ s	$1.9 \cdot 10^{-11}$ year	$3.5 \cdot 10^{8}$ s	11.29 year	273 bit
G	$4 \cdot 10^{-3}$ s	$1.3 \cdot 10^{-10}$ year	$1.1 \cdot 10^{65}$ s	$3.7 \cdot 10^{57}$ year	159 bit
S	$2 \cdot 10^{-5}$ s	$6.6 \cdot 10^{-14}$ year	**0.01** s	$3.4 \cdot 10^{-11}$ year	**10000** bit

- BF: *brute force* classical method which scans the integer numbers from 2 to $\lceil \sqrt{N} \rceil$ with complexity $O(\sqrt{N})$,
- BC: *best classical* method requiring $O(\exp[c \cdot \mathrm{ld}^{\frac{1}{3}}(N)\mathrm{ld}^{\frac{2}{3}}(\mathrm{ld}(N))])$ steps,
- G: *Grover* search based scheme with $O(N^{\frac{1}{4}})$,
- S: *Shor* factorization with $O(\mathrm{ld}(N)^3)$.

Brutális!

Multiuser detekció a Grover-algoritmusra alapozva

Dr. Imre Sándor

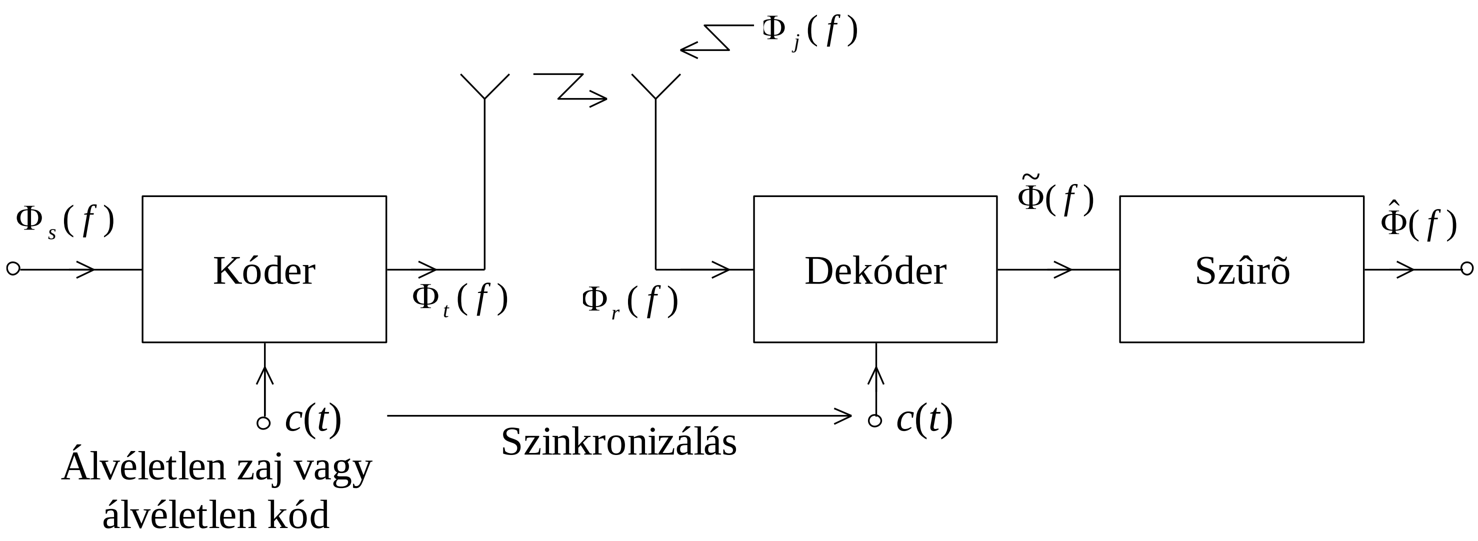
BME Hálózati Rendszerek és Szolgáltatások Tanszék

imre@hit.bme.hu

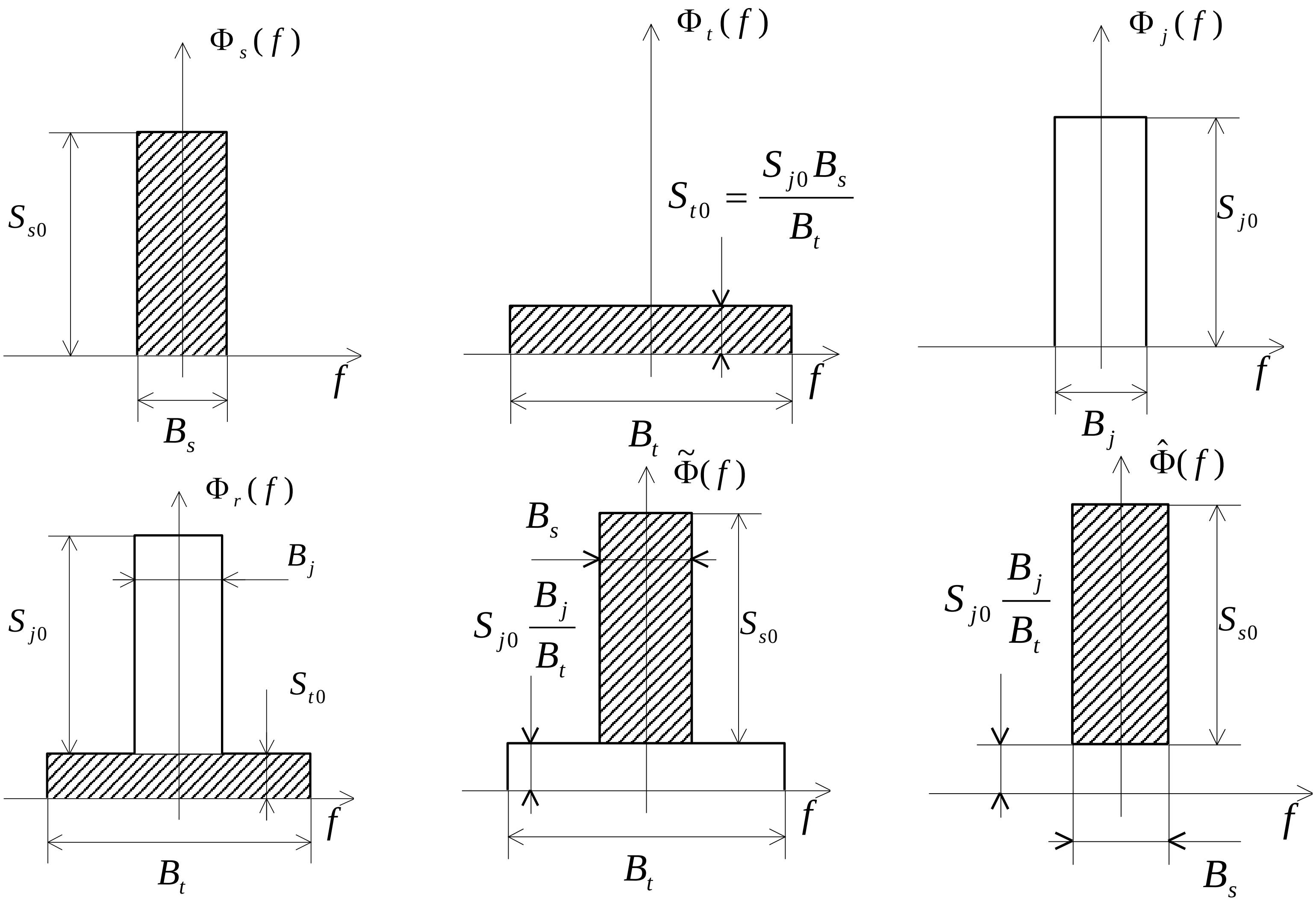
Budapest,
2025. 12. 01.

SPREAD SPECTRUM DS SS 3G MOBIL

- Gyorsan változó kód (chip) ➡ nagyfrekis komponensek



KESKENYSÁVÚ INTERFERENCIA ELNYOMÁSA



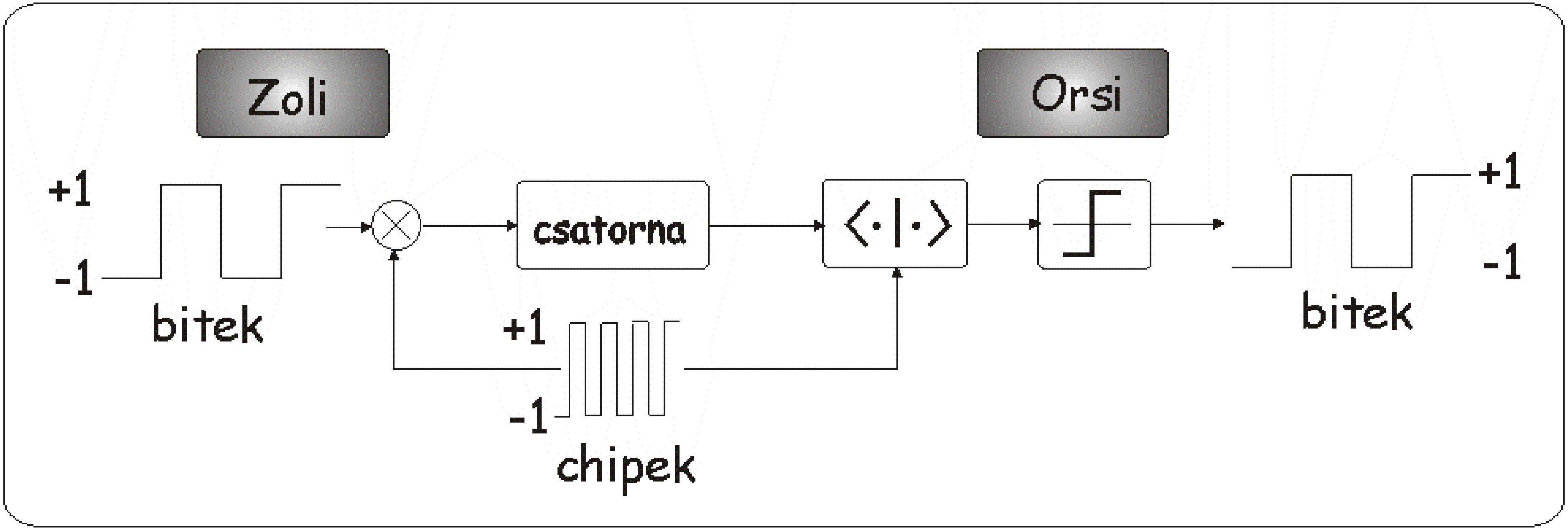
FELDOLGOZÁSI NYERESÉG

- PG: Processing Gain
- Tulajdonképpen a kiterjesztés mértéke
- PG=kiterjesztett sávszélesség/eredeti sávszélesség
- A gyakorlatban SF=chipsebesség/bitsebesség
- SF: spreading factor

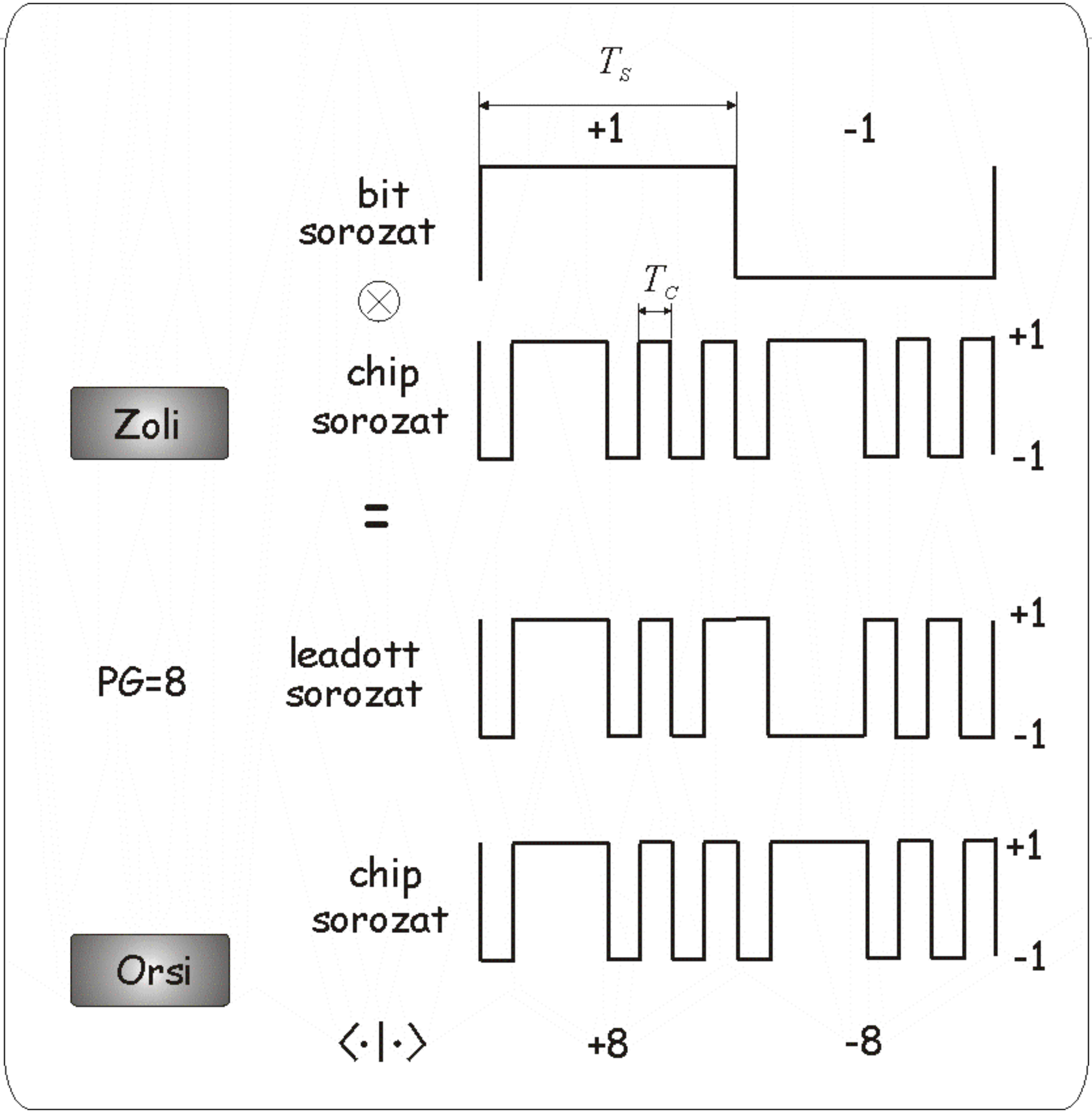
KÓDOSZTÁS

- CDMA: Code Division Multiple Access
- A spektrumkiterjesztés a felhasználókhoz rendelt ortogonális kódokkal
  - Kombinált PHY + MAC
  - Kódok ortogonalitása korlátozott

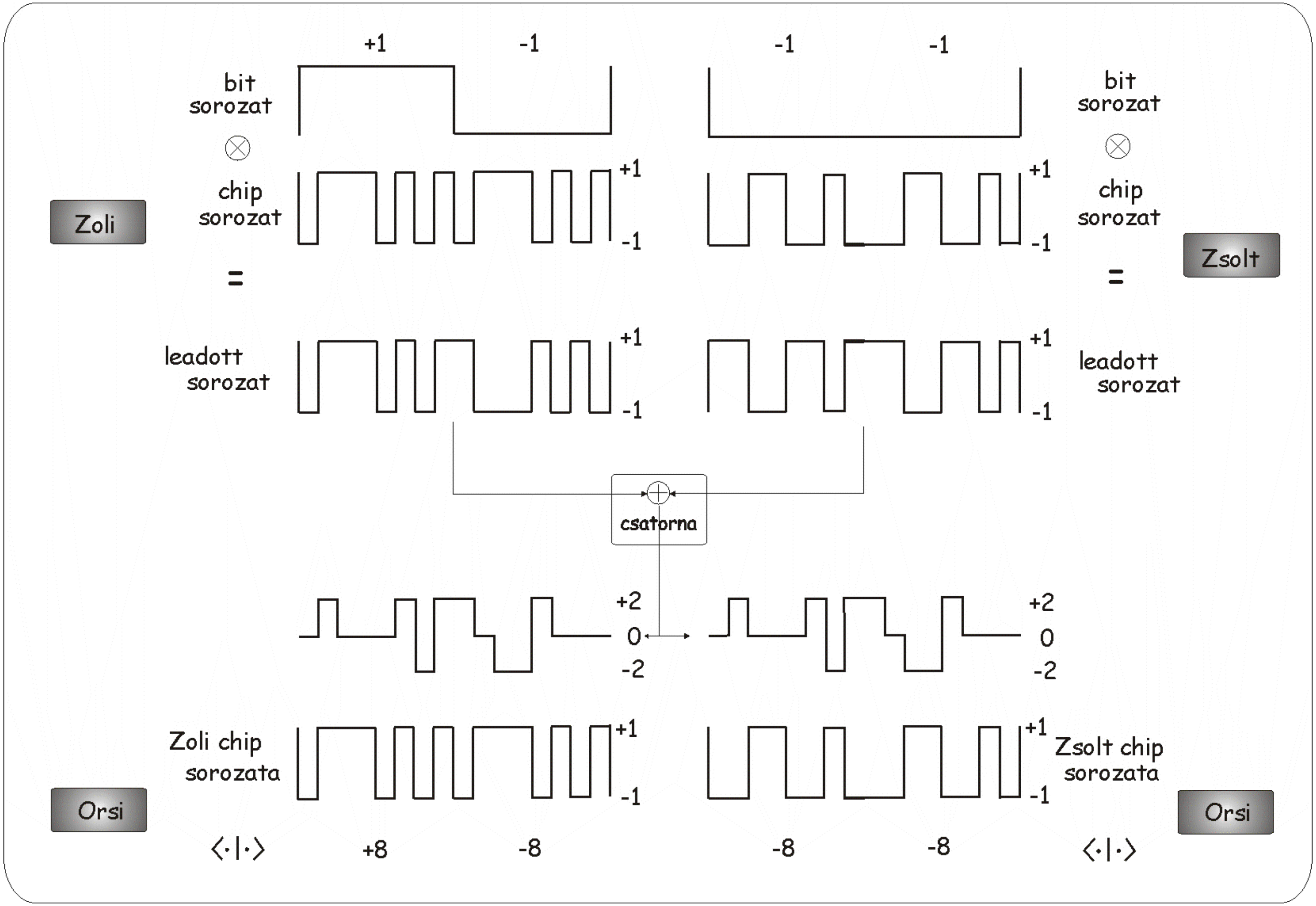
DETEKTÁLÁS



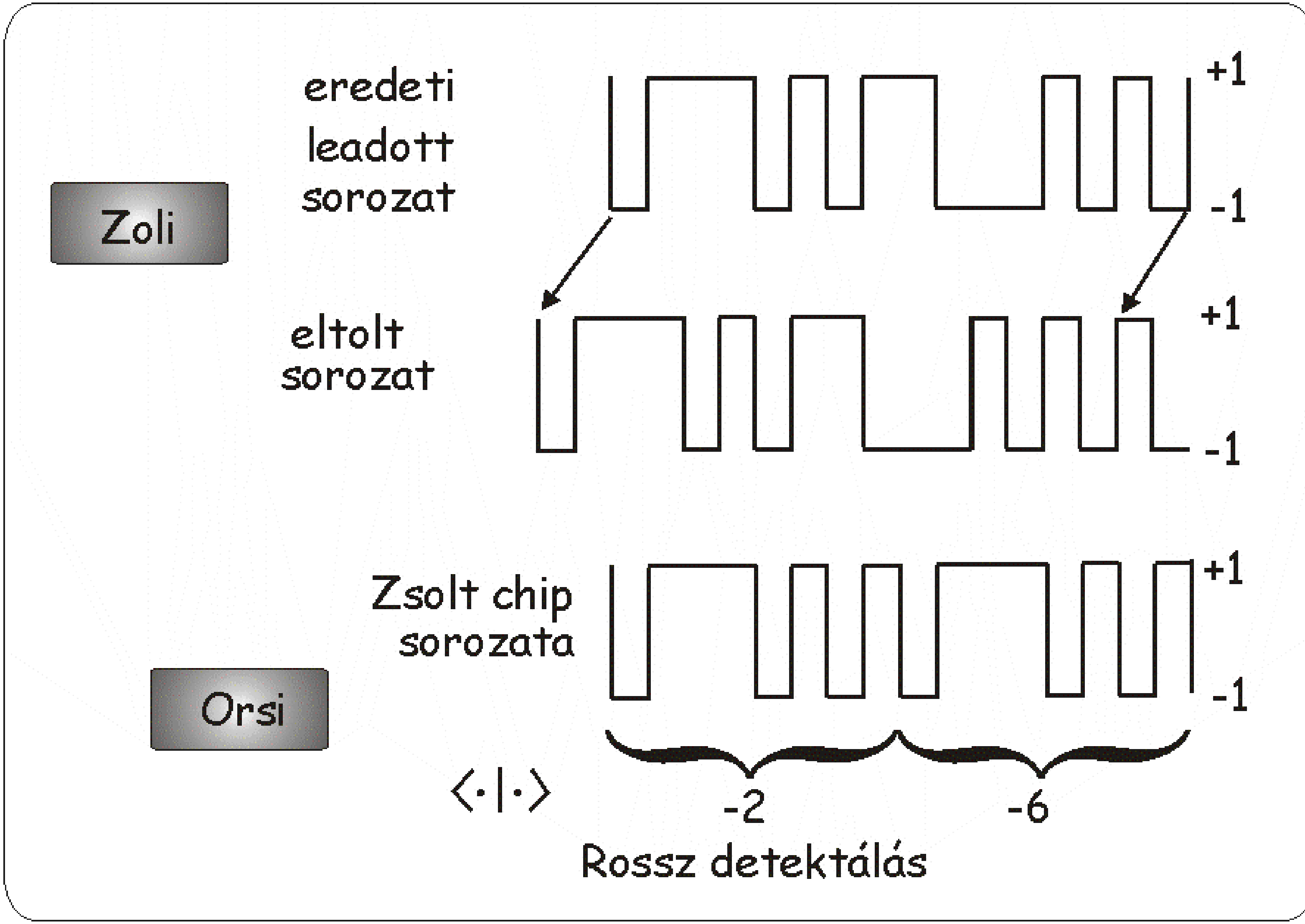
DETEKTÁLÁS


T_S
+1
-1
bit
sorozat
T_C
Zoli
chip
sorozat
+1
-1
=
PG=8
leadott
sorozat
+1
-1
chip
sorozat
+1
-1
Orsi
⟨·|·⟩
+8
-8

DETEKTÁLÁS


+1
-1
-1
-1
bit
sorozat
chip
sorozat
Zoli
+1
-1
Zsolt
=
leadott
sorozat
csatorna
+2
0
-2
Zoli chip
sorozata
Zsolt chip
sorozata
Orsi
Orsi
⟨·|·⟩
+8
-8
-8
-8

HIBA A DETEKTÁLÁS SORÁN



HÁLÓZATI RENDSZEREK ÉS SZOLGÁLTATÁSOK TANSZÉK

.hu

KVANTUM TÖBBFELHASZNÁLÓS DETEKCIÓ

- Feladat: DS-CDMA rendszerben együttes detekció a bázisállomáson.
- Vett komplex alapsávi jel $$r(t) = \sum_{k=1}^{K} \sum_{i=0}^{R} a_k[i] b_k[i] s_k(t - iT_S - \tau_k)$$

- K az egyidejűleg detektálandó felhasználók száma,
- R a börszt hossza,
- T_S a szimbólumidő,
- $a_k[i] = A_k[i]e^{j\alpha_k[i]}, \alpha_k[i] \in [0, 2\pi]; \tau_k \in [0, T_s]$ a k-dik felhasználó jelét ért komplex csatorna csillapítás és késleltetés,
- $b_k[i]$ k-dik felhasználó i-dik szimbóluma (BPSK esetén $b_k[i] \in \{+1, -1\}$),
- $s_k(t)$ a k-dik felhasználó egyedi hullámformája. $s_k(t) = \sum_{q=0}^{PG-1} c_k[q] g_k(t - qT_c)$

EGYFELHASZNÁLÓS DETEKCIÓ

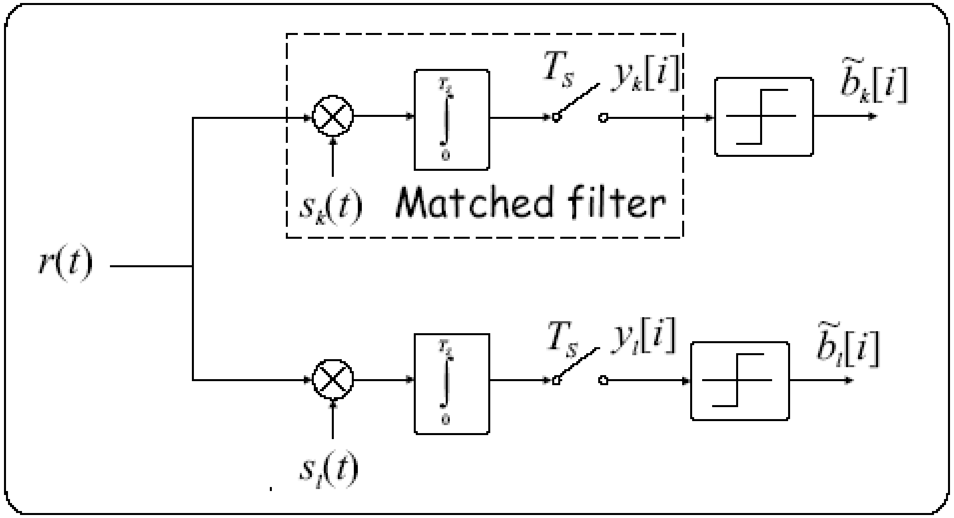
- A detektor kimenete:

$$y_k[i] = \int_0^{T_s} r(i,t)s_k(t)dt$$

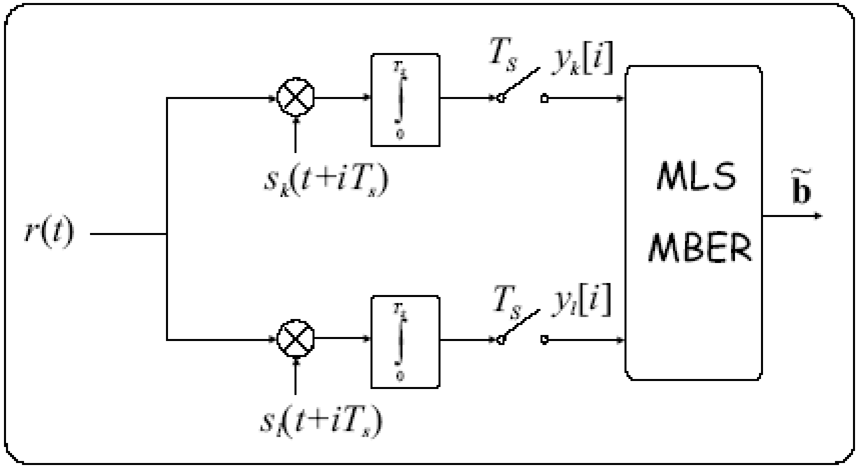
$$= \int_0^{T_s} b_k[i]s_k(t)s_k(t)dt + \int_0^{T_s} \sum_{l=1,l\neq k}^{K} b_l[i]s_l(t)s_k(t)dt = b_k[i].$$

$$\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_K] \Rightarrow B_{ik} = b_k[i], k = 1, ..., K; i = 0, ..., R,$$

$$\mathbf{Y} = [\mathbf{y}_1, \mathbf{y}_2, ..., \mathbf{y}_K] \Rightarrow Y_{ik} = y_k[i], k = 1, ..., K; i = 0, ..., R.$$



TÖBBFELHASZNÁLÓS DETEKCIÓ



- MLS, Maximum Likelihod Sequence (jointly optimum) detekció:

$$\tilde{\mathrm{B}}_{MLS} : \max_{m} f(\mathbf{Y}|\mathbf{B}_m)$$

$$H_1 : \mathbf{Y} = w(\mathbf{B}_1)$$
$$H_2 : \mathbf{Y} = w(\mathbf{B}_2)$$
$$\vdots$$
$$H_{2K(R+1)} : \mathbf{Y} = w(\mathbf{B}_{2K(R+1)})$$

- MBER, Minimum Bit Error Ratio (individually optimum) detekció:

$$\tilde{b}_k[i] : \max_{b_k[i]=\pm 1} f(y_k[i]|b_k[i]) \quad \tilde{\mathrm{B}}_{MBER} = [\tilde{b}_k[i]]$$

$$H_1 : y_k[i] = w'(b_k[i] = 1)$$
$$H_2 : y_k[i] = w'(b_k[i] = -1)$$

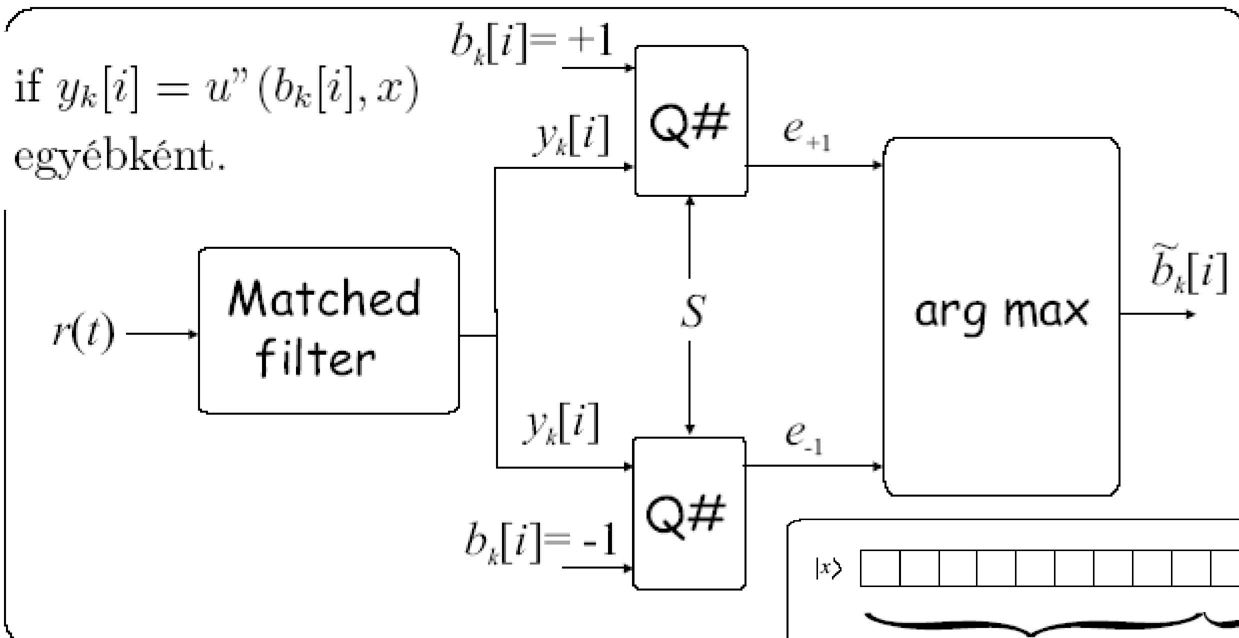
KVANTUM TÖBBFELHASZNÁLÓS DETEKCIÓ

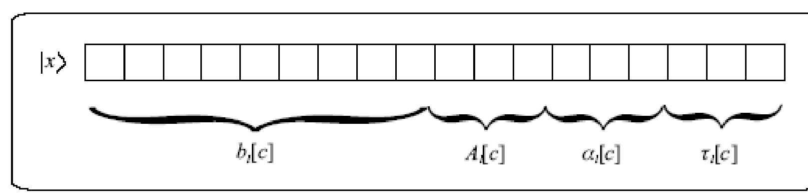
- Csatorna mátrix: $\mathbf{Z}_{\pm 1} = [\mathbf{B}_{\pm 1}, \mathbf{A}, \mathbf{C}, \mathbf{d}]$

$$\mathbf{A} : A_{ik} = A_k[i]; \mathbf{C} : C_{ik} = \alpha_k[i]; \mathbf{d} : d_k = \tau_k$$

$$f(y_k[i] | b_k[i] = \pm 1) = \frac{\#(\mathbf{Z}_{\pm 1} : y_k[i] = u'(\mathbf{Z}_{\pm 1}))}{\#(\mathbf{Z}_{\pm 1})}$$

$$f(x) = \begin{cases} 1 & \text{if } y_k[i] = u"(b_k[i], x) \\ 0 & \text{egyébként.} \end{cases}$$





KVANTUM TÖBBFELHASZNÁLÓS DETEKCIÓ

- Komplexitás:

$$n^{\clubsuit} = n + \left\lceil \mathrm{ld}(2\pi) + \mathrm{ld}\left(3 + \frac{1}{\breve{P}_{\varepsilon}}\right)\right\rceil$$

$$n = K(R+1)(n_A + n_\alpha + 1) + Kn_\tau - 1$$

2.3. tézis: Kvantum alapú többfelhasználós detekció DS-CDMA rendszerekben (5. fejezet)

Megmutattam, hogy az optimális többfelhasználós detekciós eljárás – mely klasszikusan nagy számításigényű feladat – miként vezethető vissza kvantum fázisbecslésre, jelentősen csökkentve a számítási komplexitást. Megadtam a vonatkozó kvantum architektúrat is. [1,4,6]

HÁLÓZATI RENDSZEREK
ÉS SZOLGÁLTATÁSOK
TANSZÉK

Kvantum egzisztencia/reláció tesztelés és szélsőérték keresés

Dr. Imre Sándor

BME Hálózati Rendszerek és Szolgáltatások Tanszék

imre@hit.bme.hu

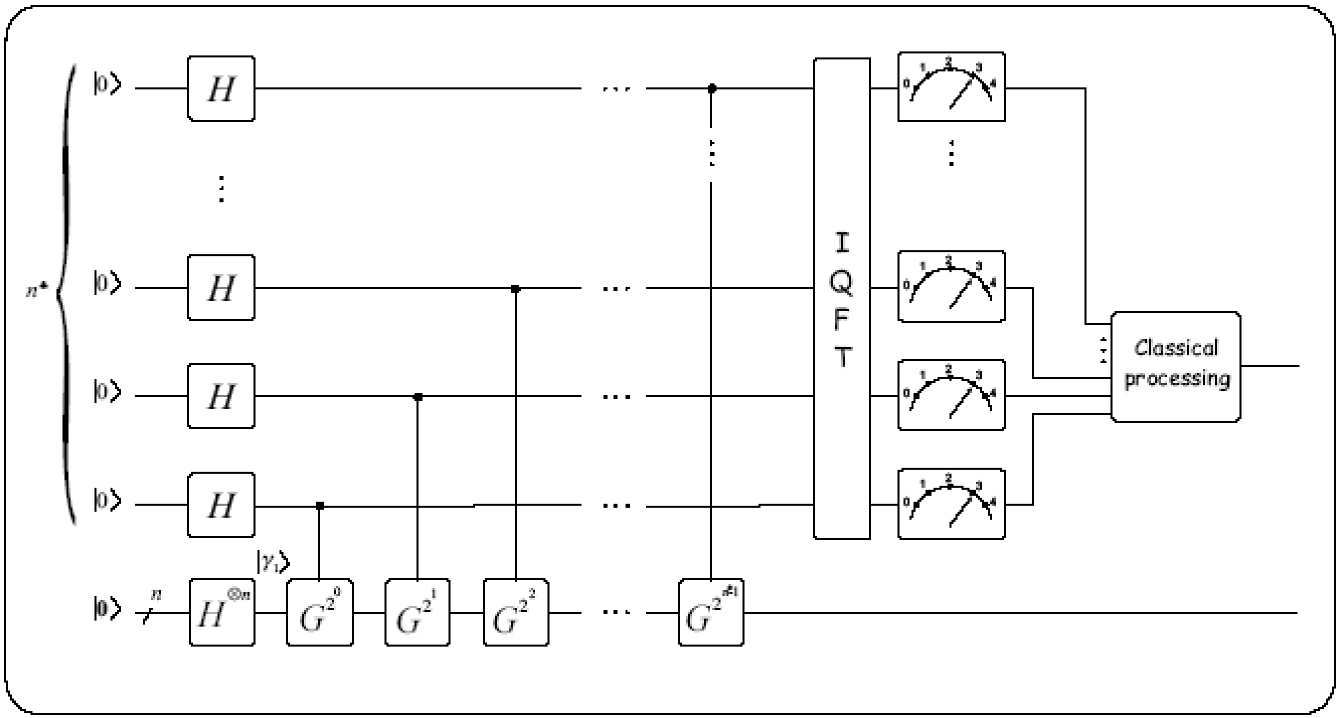
Budapest,
2025. 12. 01.

MŰEGYETEM 1782

KVANTUM EGZISZTENCIA TESZTELÉS

- Cél: annak eldöntése, hogy a keresett elem egyáltalán előfordul-e az adatbázisban?
- Klasszikus bonyolultság: $O(N)$.
- Speciális fázisbecslés a Grover-operátoron.
- Fázisbecslés:
  - Unitér operátor sajátértéke: $U\left|u\right\rangle = e^{j\alpha_u}\left|u\right\rangle$
  - Fázis: $\alpha_u = 2\pi\kappa_u$.
  - Fázistényező közelítése: $\kappa_u = i/2^n$

KVANTUM FÁZISBECSLÉS - KOMPLEXITÁS



$$e^{j\alpha_u}$$

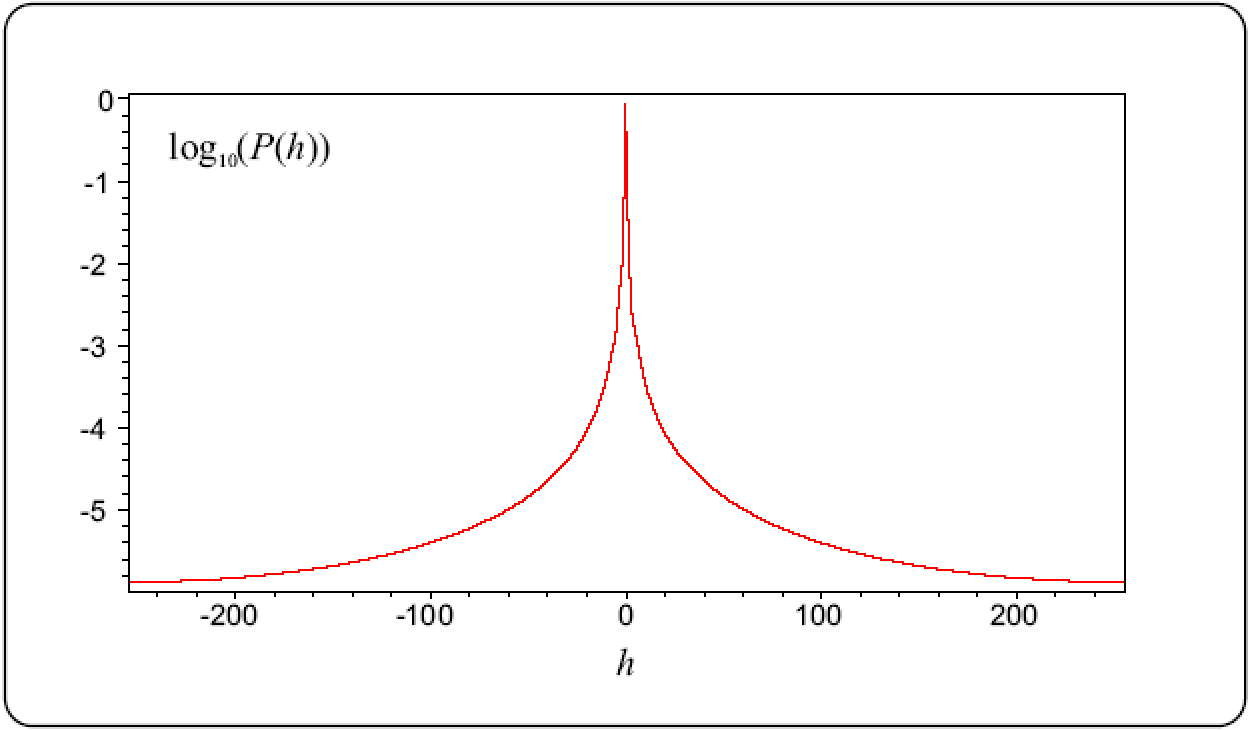
$$n^{\clubsuit} = c - 1 + \left\lceil \mathrm{ld}(2\pi) + \mathrm{ld}\left(3 + \frac{1}{\breve{P}_{\varepsilon P}}\right) \right\rceil$$

p qbit

Klasszikus bizonytalanság 2^{-c}

Kvantum bizonytalanság

KVANTUM BIZONYTALANSÁG



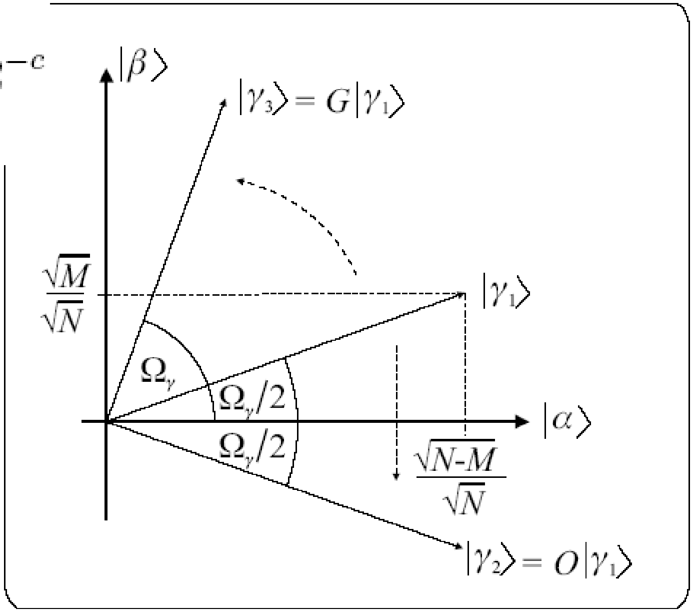
KVANTUM EGZISZTENCIA TESZTELÉS

- Klasszikus bizonytalanság:

Thus the worst-case scenario occurs when $\frac{\Omega_\gamma}{2}$ is the smallest, that is we have the smallest angle between $|\gamma_1\rangle$ and $|\alpha\rangle$. Hence the classical accuracy c should be chosen such that in the case $M = 1$ the measured output of the IQFT contains at least one nonzero bit which allows distinguishing it from $|\mathbf{0}\rangle$. Let us assume again without loss of generality that we have a database $N = 2^n$ entry of size, therefore using (7.20) we need

$$\min(\Omega_\gamma) = 2\arcsin\left(\sqrt{\frac{1}{N}}\right) \cong 2\sqrt{\frac{1}{N}} = 2^{(-n/2+1)} \geq 2^{-c}$$

$$c = \left\lceil \frac{n}{2} \right\rceil - 1$$



- Komplexitás:

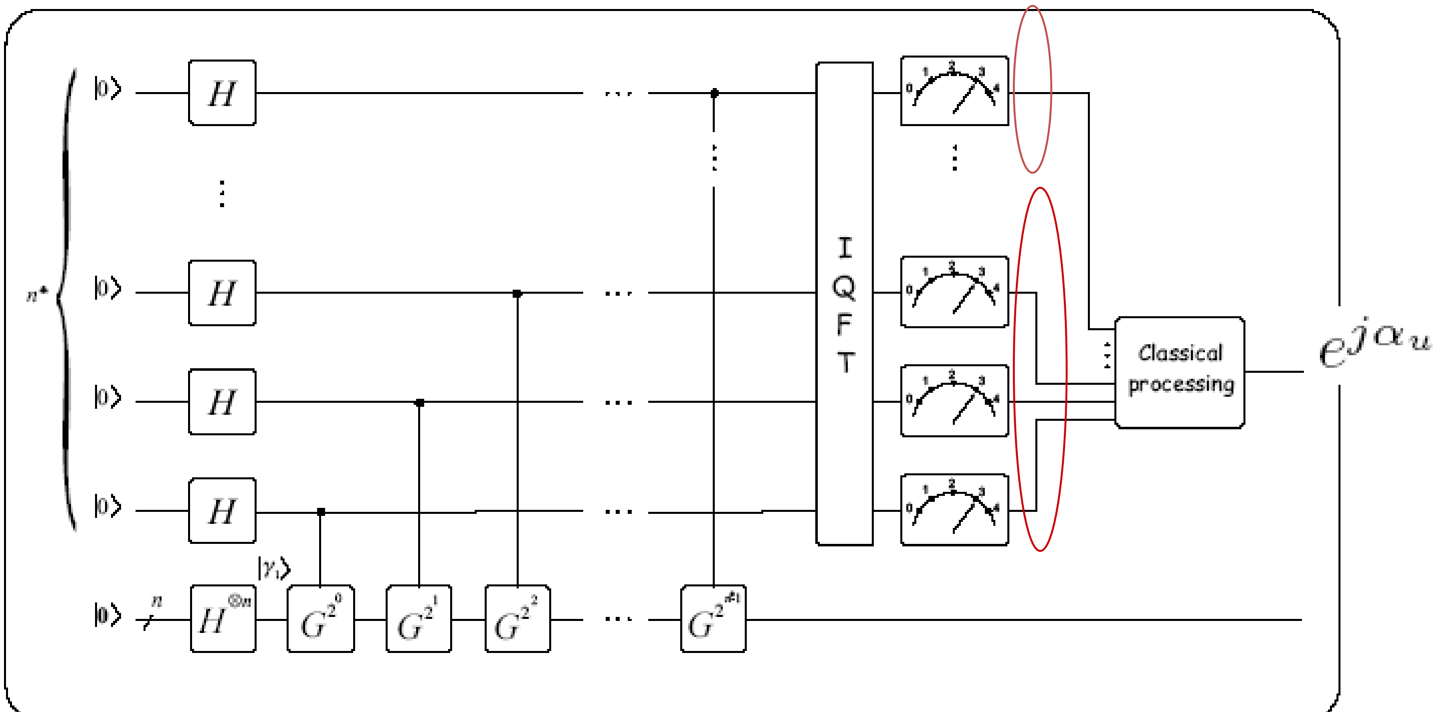
$$n^\clubsuit = \left\lceil \frac{n}{2} + \mathrm{ld}(2\pi) + \mathrm{ld}\left(3 + \frac{1}{\breve{P}_{\varepsilon P}}\right) \right\rceil$$

KVANTUM BIZONYTALANSÁG

$$P_{\varepsilon E} = \underbrace{P(\tilde{\Omega}_\gamma \neq 0 | \Omega_\gamma = 0)}_{\equiv 0} P(\Omega_\gamma = 0) + \sum_{\Omega_\gamma \neq 0} P(\tilde{\Omega}_\gamma = 0 | \Omega_\gamma) P(\Omega_\gamma)$$

It is easy to see that if $M = 0$ then $\Omega_\gamma = 0$ is measured *always* with certainty since the phase ratio $\kappa = \Omega_\gamma / 2\pi$ is also equal to zero, which corresponds to the idealistic phase estimation

- Hiba, ha $\Omega_\gamma \neq 0$ és az $n^\clubsuit - p$ MSB biten csupa 0 érték van.



KVANTUM BIZONYTALANSÁG

- Kvantum bizonytalanság:

$$\breve{P}_\varepsilon \geq P_{\varepsilon E} = \sum_{i=0}^{2^p-1} \left| \frac{1}{2^{n^\clubsuit}} \frac{1-e^{j2\pi\left(2^{n^\clubsuit}\frac{\Omega\gamma}{2\pi}-i\right)}}{1-e^{j2\pi\left(\frac{\Omega\gamma}{2\pi}-\frac{i}{2^{n^\clubsuit}}\right)}} \right|^2$$

- Komplexitás:

Egzisztencia tesztelés

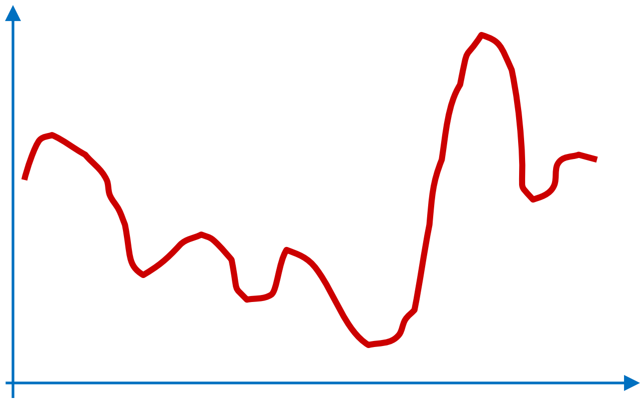
$$n^\clubsuit = \left\lceil \frac{n}{2} + \mathrm{ld}(2\pi) + \underbrace{\mathrm{ld}\left(\frac{1}{8\breve{P}_\varepsilon}\right)}_{p} \right\rceil$$

Kvantum számlálás (fázisbecslés)

$$n^\clubsuit = \left\lceil \frac{n}{2} + \mathrm{ld}(2\pi) + \mathrm{ld}\left(3 + \frac{1}{\breve{P}_{\varepsilon P}}\right) \right\rceil$$

KVANTUM SZÉLSŐÉRTÉK KERESÉS

- Klasszikus rendezetlen adatbázis

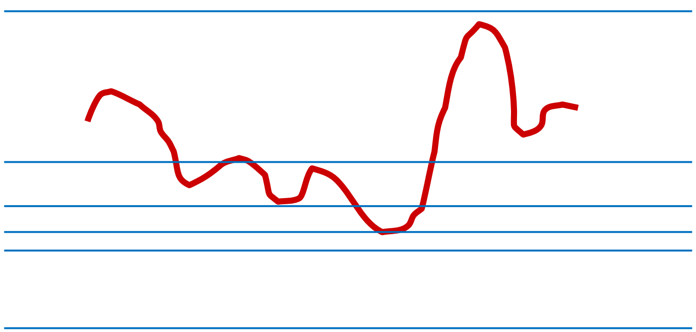


- Rendezés + Logaritmusos keresés
- A rendezés nem mindig tehető meg!
- A klasszikus logaritmusos keresés kombinálása kvantum egzisztencia teszteléssel

KVANTUM SZÉLSŐÉRTÉK KERESÉS

- Adatbázis (függvény!): $y = g[x] \quad x \in [0, N-1] \quad y \in [G_{\min 0}, G_{\max 0}]$
- Feladat: $\min_x(g[x]) = g[x_{opt}] = y_{opt}$
- A kereső algoritmus:

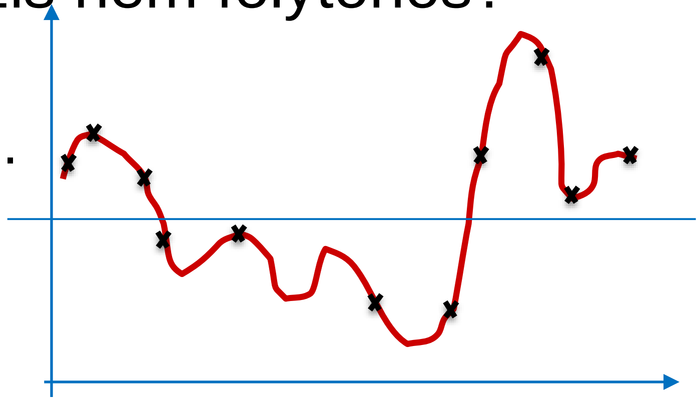
1. $s = 0$: $G_{\min 1} = G_{\min 0}$, $G_{\max 1} = G_{\max 0}$ and $\Delta G = G_{\max 0} - G_{\min 0}$
2. $s = s + 1$
3. $G_{\mathrm{med}s} = G_{\min s} + \left\lceil \frac{G_{\max s} - G_{\min s}}{2} \right\rceil$
4. $flag = QET(G_{\mathrm{med}s})$
   - Ha $flag = YES$ akor $G_{\max s+1} = G_{\mathrm{med}s}$, $G_{\min s+1} = G_{\min s}$
   - egyébként $G_{\max s+1} = G_{\max s}$, $G_{\min s+1} = G_{\mathrm{med}s}$.
5. Ha $s < \mathrm{ld}(\Delta G)$ akkor vissza a 2-es ponthoz, egyébként leállás és $y_{opt} = G_{\mathrm{med}s}$.



- Grover kereséssel: $x_{opt} = g^{-1}[y_{opt}]$.
- Komplexitás: $\boxed{O(\mathrm{ld}(\Delta G)\mathrm{ld}^3(\sqrt{N}))}$

KVANTUM SZÉLSŐÉRTÉK KERESÉS

- Probléma: mi történik, ha az adatbázis nem folytonos?
  - Akár így állították össze
  - Akár feltételes optimizálás esete áll fenn.



- Kvantum reláció tesztelés! (≥,≤,>,<,=)
  - Van-e adott tulajdonságú elem az adatbázisban?
- Praktikusan ennek alesete az egzisztencia tesztelés (=)

ERŐFORRÁS OPTIMALIZÁLÁS – A KIHÍVÁS

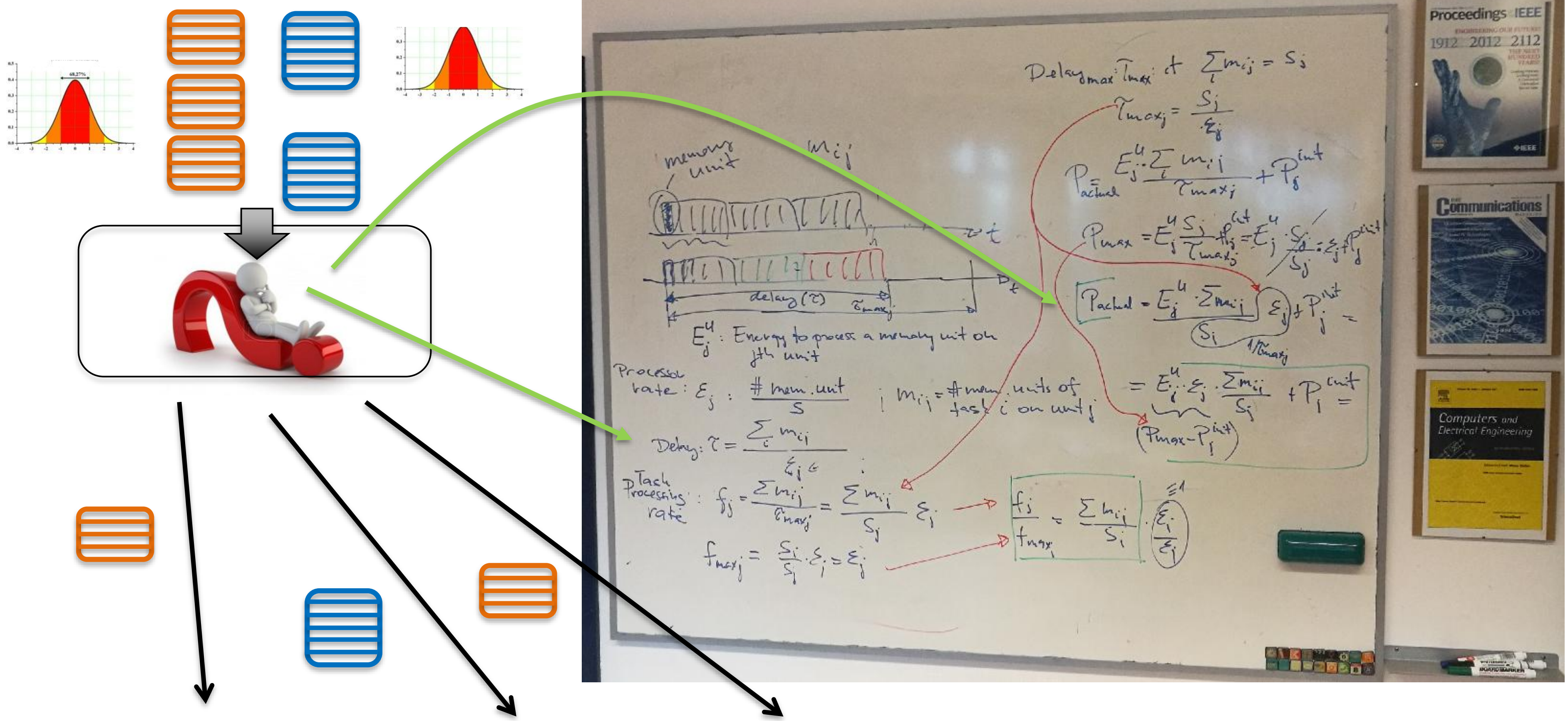
- Központosított
  - Adattárolás
  - Feldolgozás
  - 5G mobil hálózatok!
- Erőforrás kezelés optimalizálása
  - Több egyidejűleg kiszolgálható feladat
  - Kisebb energiafelhasználás
  - Szigorúbb késleltetési követelmények

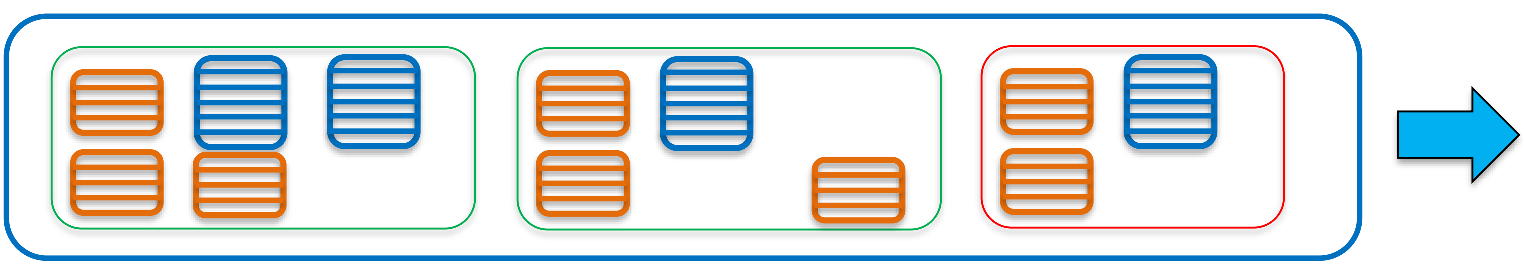

ANGKOR DATA COMMUNICATIONS GROUP CO., LTD


Sara El Gaily


Microsoft

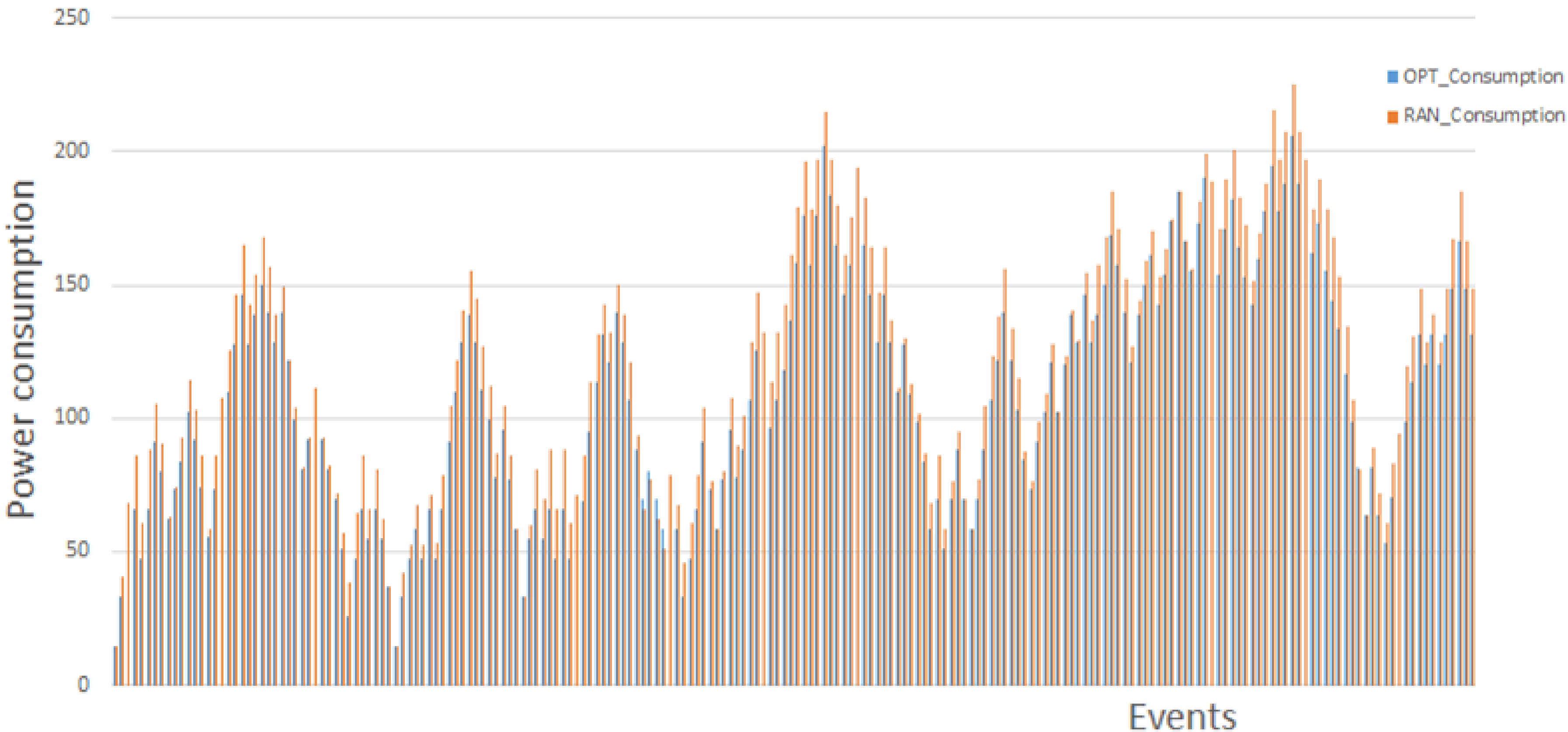
ERŐFORRÁS OPTIMALIZÁLÁS – MODELL: FELTÉTELES OPTIMALIZÁLÁS





Keresés az összes lehetséges megoldás terében!

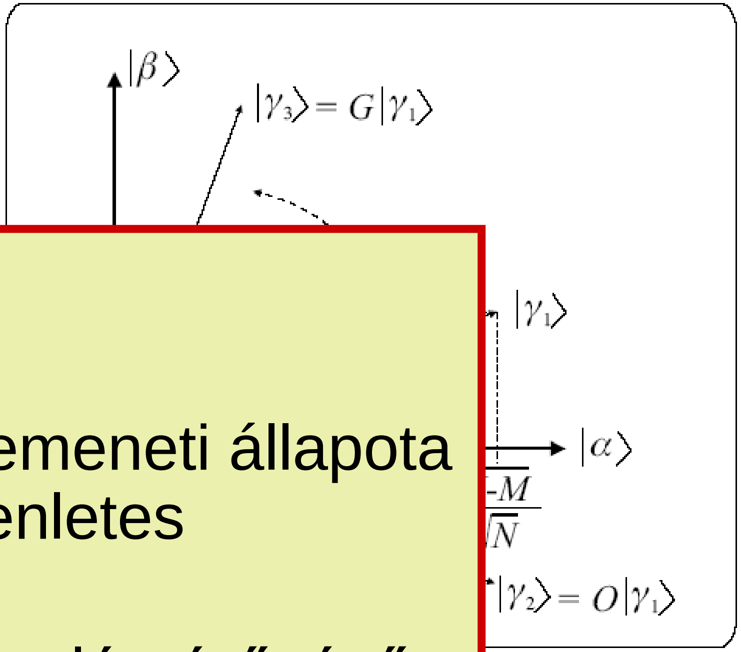
ERŐFORRÁS OPTIMALIZÁLÁS

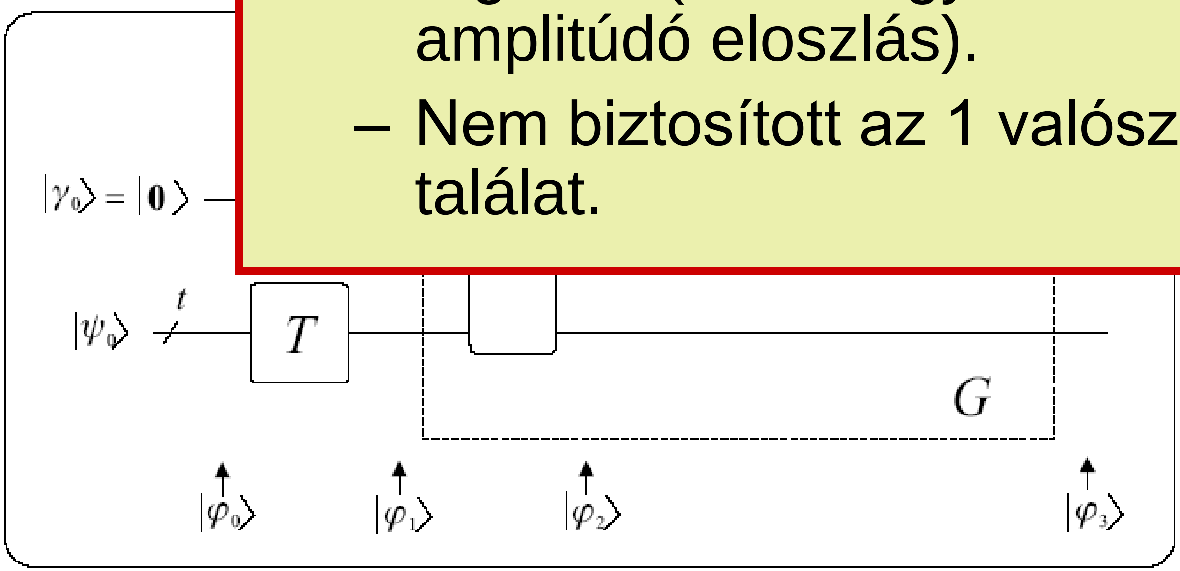


ALAP GROVER-ALGORITMUS

$$L_{opt} = \lfloor \hat{l}_0 \rceil = \left\lfloor \frac{\frac{\pi}{2} - \frac{\Omega_\gamma}{2}}{\Omega_\gamma} \right\rceil$$

P_ε





- A Grover-algoritmus hiányosságai:
  - Az index regiszter bemeneti állapota rögzített (valós, egyenletes amplitúdó eloszlás).
  - Nem biztosított az 1 valószínűségű találat.

ÁLTALÁNOSÍTOTT GROVER-ALGORITMUS

- 2-dimenziós bázis a *V* térben:

$$|\alpha\rangle = \frac{1}{\sqrt{\sum_{x\in\overline{S}} |\gamma_{1x}|^2}} \sum_{x\in\overline{S}} \gamma_{1x}|x\rangle$$

$$|\beta\rangle = \frac{1}{\sqrt{\sum_{x\in S} |\gamma_{1x}|^2}} \sum_{x\in S} \gamma_{1x}|x\rangle$$

Egyes speciális állapotok nem képezhetők le.

- Általánosított Grover-operátor:

$$G \triangleq HPHO$$

$$H \to U,$$

$$O \to I_\beta \triangleq I + \left(e^{j\phi} - 1\right) \sum_{x\in S} |x\rangle\langle x|,$$

$$P \to I_\eta \triangleq I + \left(e^{j\theta} - 1\right) |\eta\rangle\langle\eta|.$$

$$Q = -\left(I + \left(e^{j\theta} - 1\right)|\mu\rangle\langle\mu|\right) I_\beta \qquad |\mu\rangle \triangleq U|\eta\rangle$$

MEGHATÁROZANDÓ PARAMÉTEREK

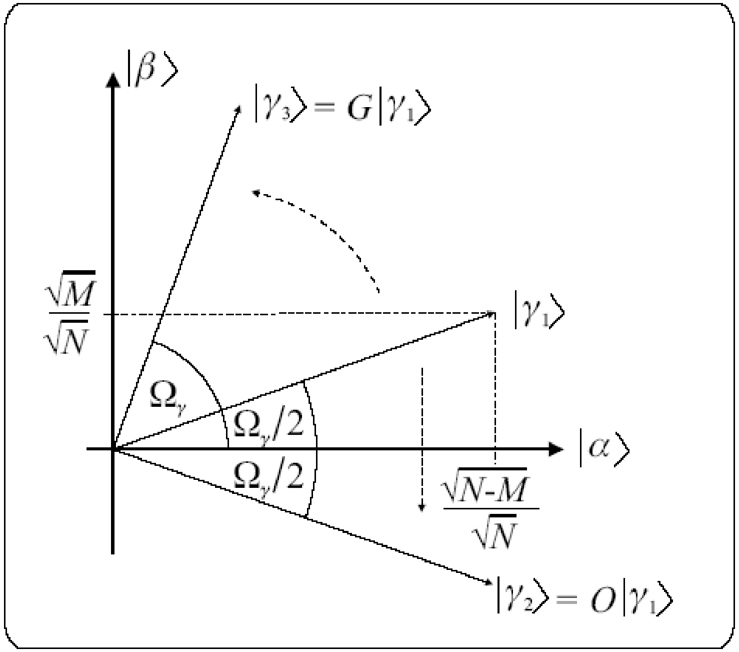
$$|\mu\rangle \triangleq U|\eta\rangle \quad \rightarrow \quad |\mu\rangle = \cos(\Omega)|\alpha\rangle + \sin(\Omega)\, e^{j\Lambda}|\beta\rangle$$

$|\alpha\rangle$ és $|\beta\rangle$ nem ismert!

$$|\gamma_1\rangle = \cos\left(\frac{\Omega_\gamma}{2}\right)|\alpha\rangle + \sin\left(\frac{\Omega_\gamma}{2}\right) e^{j\Lambda_\gamma}|\beta\rangle$$

$$I_\beta \triangleq I + (e^{j\phi} - 1)\sum_{x \in S} |x\rangle\langle x|$$

$$I_\eta \triangleq I + (e^{j\theta} - 1)\,|\eta\rangle\langle\eta|$$



ÁLTALÁNOSÍTOTT GROVER-OPERÁTOR

- Q alakja a V 2-dimenziós térben
  - Feltétel: $|\mu\rangle \triangleq U|\eta\rangle$ legyen az $|\alpha\rangle$, $|\beta\rangle$ térben.
  - Q megőrzi a teret.
- Q sajátértékei:

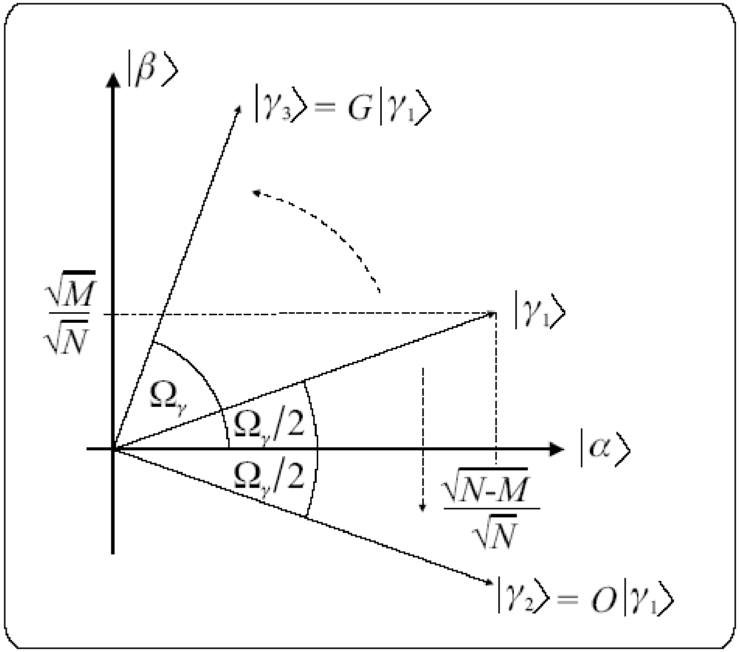
$$\mathbf{G} = \begin{bmatrix} \cos(\Omega_\gamma) & -\sin(\Omega_\gamma) \\ \sin(\Omega_\gamma) & \cos(\Omega_\gamma) \end{bmatrix} \rightarrow e^{\pm j\Omega_\gamma}$$

$$Q = -\begin{bmatrix} e^{j\theta}\cos^2(\Omega) + \sin^2(\Omega) & e^{j\phi}e^{-j\Lambda}\left(e^{j\theta}-1\right)\frac{\sin(2\Omega)}{2} \\ \left(e^{j\theta}-1\right)e^{j\Lambda}\frac{\sin(2\Omega)}{2} & e^{j\phi}\left[e^{j\theta}\sin^2(\Omega)+\cos^2(\Omega)\right] \end{bmatrix}$$

$$Q|\psi_{1,2}\rangle = q_{1,2}|\psi_{1,2}\rangle \rightarrow q_{1,2} = -e^{j\left(\frac{\theta+\phi}{2}\pm\Upsilon\right)}$$

$$\cos(\Upsilon) = \cos\left(\frac{\theta-\phi}{2}\right) + \sin^2(\Omega)\left(\cos\left(\frac{\theta+\phi}{2}\right) - \cos\left(\frac{\theta-\phi}{2}\right)\right)$$

LÉPÉSSZÁM



$$\boxed{\langle\alpha|Q^{l_s}|\gamma_1\rangle = 0}$$

$$\Im\left\{\langle\alpha|Q^{l_s}|\gamma_1\rangle\right\} = 0$$

Illesztési feltétel:

$$\tan\left(\frac{\phi}{2}\right) = \frac{\cos(2\Omega) + \sin(2\Omega)\cdot\tan\left(\frac{\Omega_\gamma}{2}\right)\cos(\Lambda - \Lambda_\gamma)}{\cot\left(\frac{\theta}{2}\right) - \tan\left(\frac{\Omega_\gamma}{2}\right)\sin(2\Omega)\sin(\Lambda - \Lambda_\gamma)}$$

$$\Re\left\{\langle\alpha|Q^{l_s}|\gamma_1\rangle\right\} = 0$$

Lépésszám:

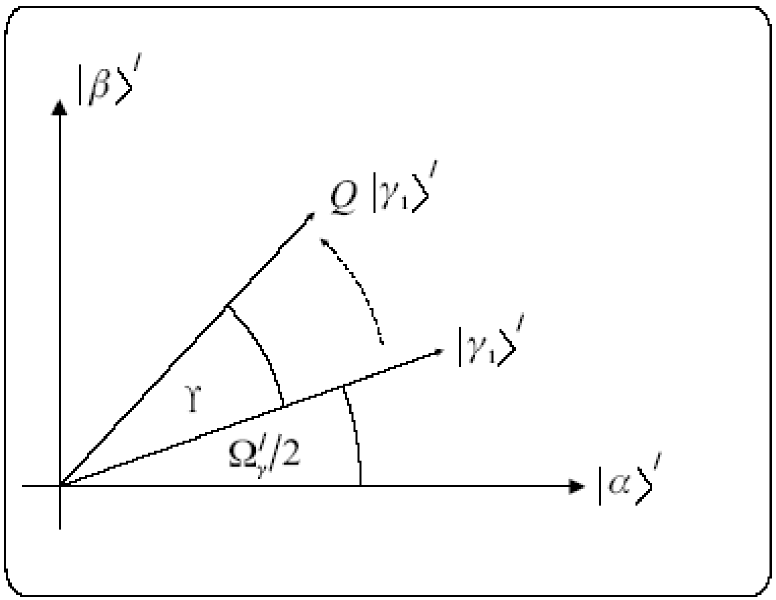
$$l_s = \frac{\frac{\pi}{2} - \left|\arcsin\left(\sin\left(\frac{\phi(\theta)}{2} - \Lambda + \Lambda_\gamma\right)\sin\left(\frac{\Omega_\gamma}{2}\right)\right)\right|}{\Upsilon}$$

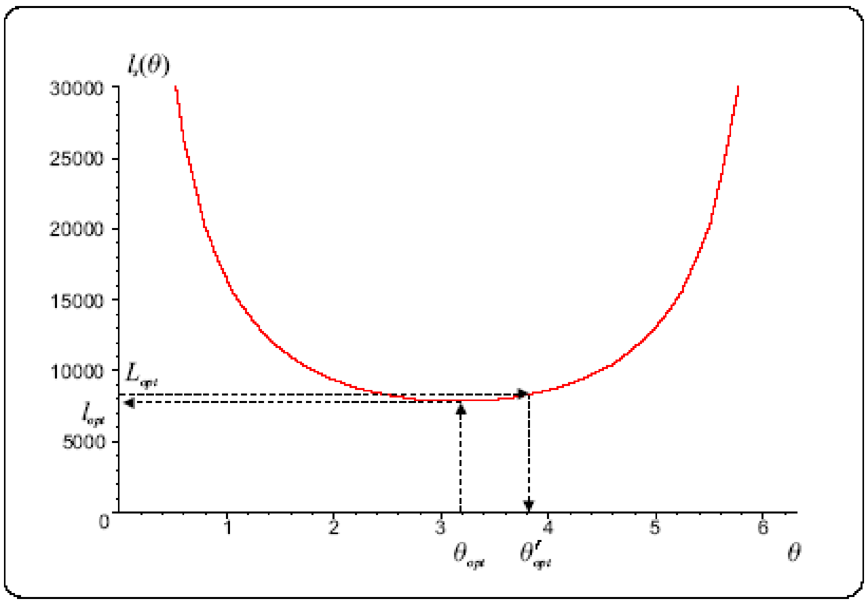
OPTIMÁLIS LÉPÉSSZÁM

$$L_{opt} = \lfloor \hat{l}_0 \rceil = \left\lfloor \frac{\frac{\pi}{2} - \frac{\Omega_\gamma}{2}}{\Omega_\gamma} \right\rceil$$

- Az 1 valószínűségű találathoz szükséges lépésszám:

$$\Omega_\gamma \rightarrow \quad l_s = \frac{\frac{\pi}{2} - \left| \arcsin\left(\sin\left(\frac{\phi(\theta)}{2} - \Lambda + \Lambda_\gamma\right)\sin\left(\frac{\Omega_\gamma}{2}\right)\right)\right|}{\Upsilon}$$





- Spec. eset: eredeti Grover-algoritmus, optimális, mert kevesebb lépésből nem lehet célba érni!

BEÁLLÍTÁSOK

$$\cos(\Upsilon) = \cos\left(\frac{\theta-\phi}{2}\right) + \sin^2(\Omega)\left(\cos\left(\frac{\theta+\phi}{2}\right) - \cos\left(\frac{\theta-\phi}{2}\right)\right)$$

$$q_{1,2} = -e^{j\left(\frac{\theta+\phi}{2}\pm\Upsilon\right)}$$

Fázisbecslés

$O(\mathrm{ld}^3(N))$

$$\theta = \phi = \pi$$

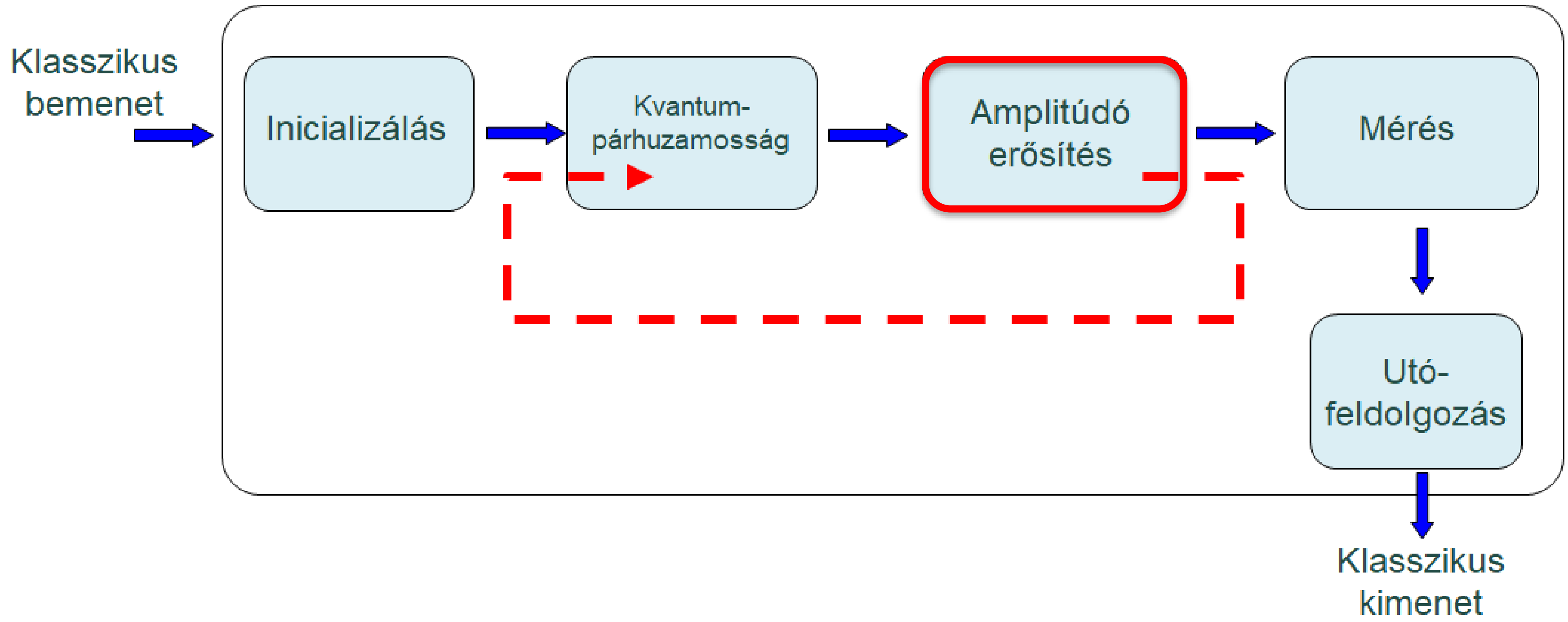
$$\Upsilon \rightarrow \Omega \rightarrow \Omega_\gamma$$

$$|\mu\rangle = |\gamma_1\rangle \rightarrow \Lambda = \Lambda_\gamma \quad \Omega = \frac{\Omega_\gamma}{2}$$

U := a $|\gamma_1\rangle$ létrehozásához szükséges kapuk összessége

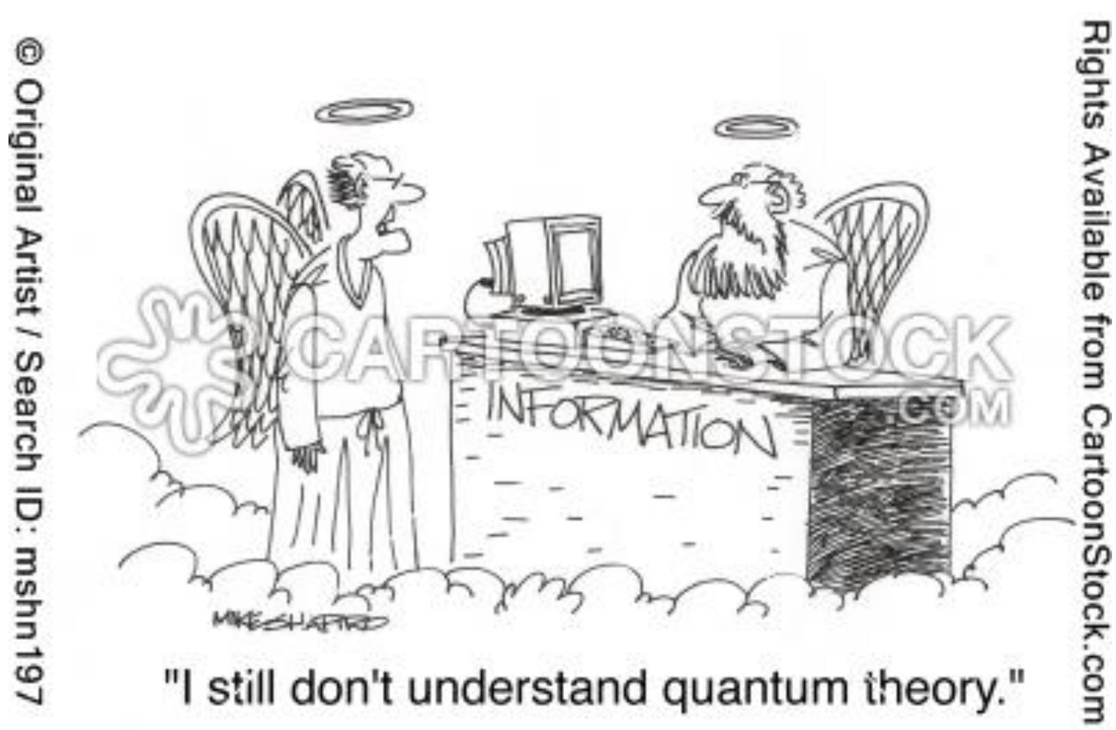
$|\eta\rangle$:= a felhasználó indító klasszikus állapota

AMPLITÚDÓ ERŐSÍTÉS



AMPLITÚDÓ ERŐSÍTÉSI TECHNIKÁK

- Hadamard-kapu, pl. Deutsch-Jozsa-algoritmus
- Adott az amplitúdó erősites pl. IQFT és ehhez keresünk párhuzamossagot, pl. fazisbecslés
- Megnézzuk a párhuzamosság sajátértékeit és ha lehet fázisbecslésre vezetjük vissza, pl. rendkeresés, kvantumos számlálás, reláció tesztelés
- Itetatív, pl. Grover-algoritmus


© Original Artist / Search ID: mshn197
INFORMATION
CARTOONSTOCK.COM
"I still don't understand quantum theory."
Rights Available from CartoonStock.com