DEPARTMENT OF NETWORKED SYSTEMS AND SERVICES




# Searching in an Unsorted Database

"Man - a being in search of meaning."

Plato

**Márton Czermann**

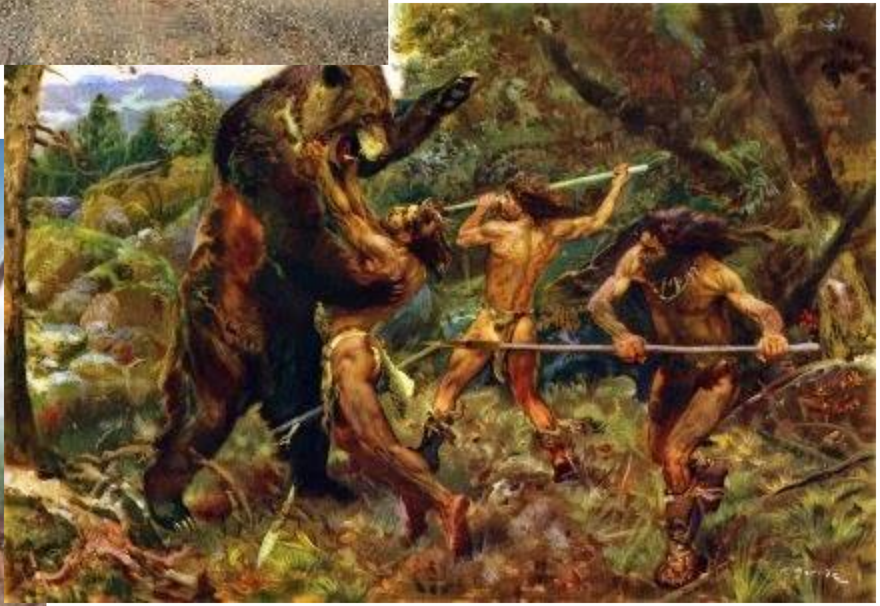
Mobile Communications and Quantum Technologies Lab

czermann@mcl.hu

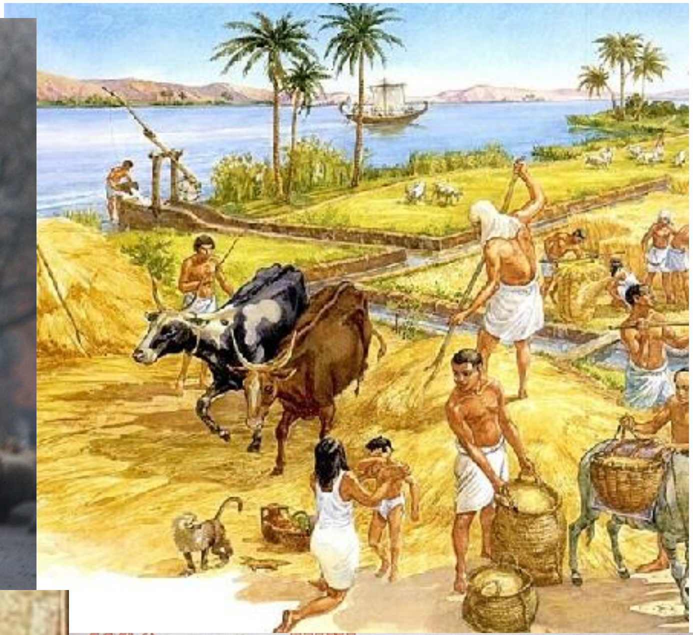
Budapest,
2025. 05. 11.

DEPARTMENT OF
NETWORKED SYSTEMS
AND SERVICES

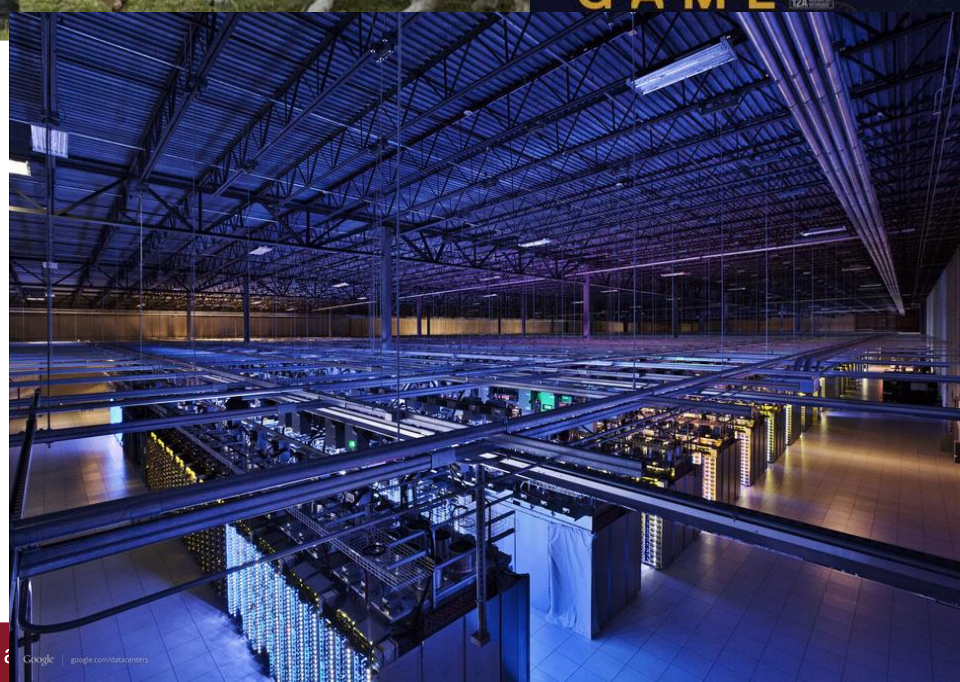
# HISTORY OF DATA BASE SEARCHING V1



# HISTORY OF DATA BASE SEARCHING V2



# HISTORY OF DATA BASE SEARCHING V3

# OBJECTIVES

- Finding a certain entry in a database $N$ items of size.
- The DB is unsorted.
- The DB contains $M$ copy of the requested entry.
- Best classical solution: $N$ questions.
- How can be exploited quantum phenomena ?

elements/items

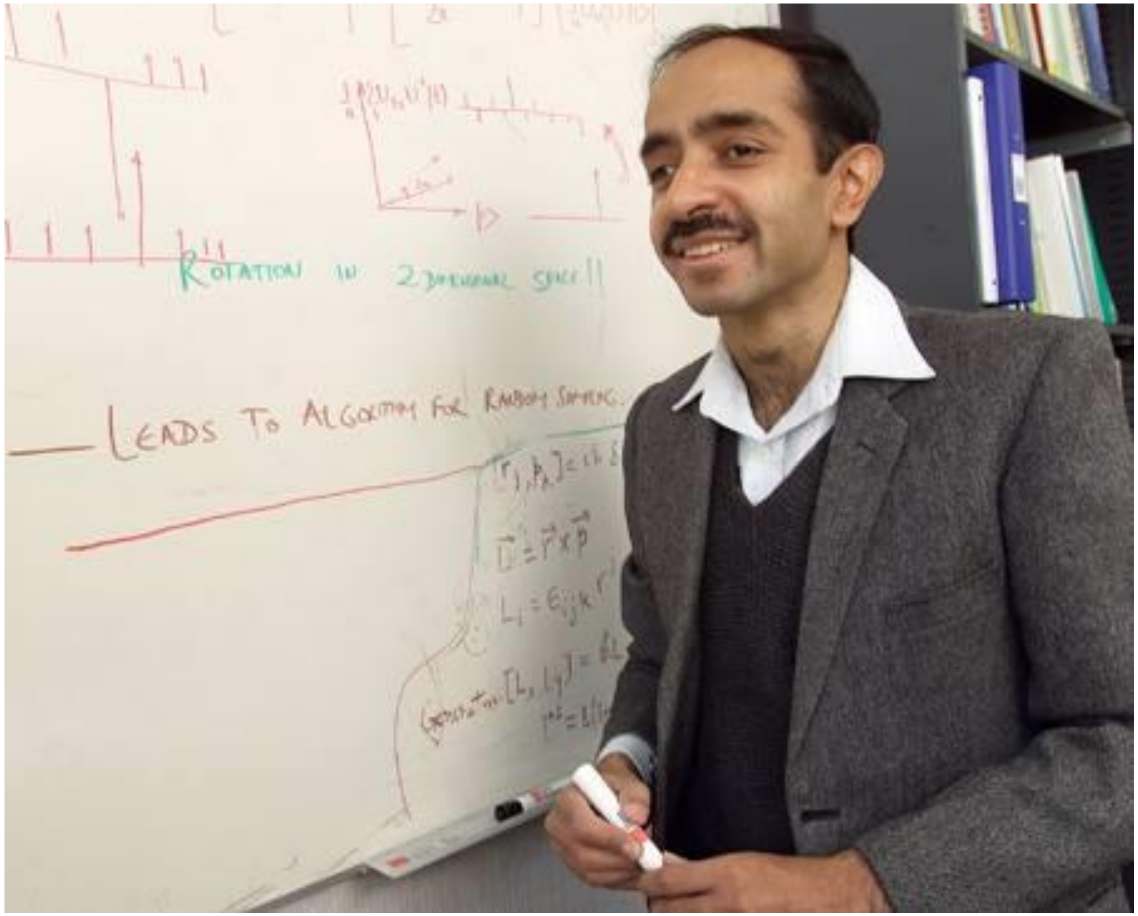
| Data base: greengrocer's | |
|---|---|
| 0 | apple |
| 1 | banana |
| 2 | tomato |
| 3 | carrot |
| 4 | potato |
| 5 | raspberry |
| 6 | onion |
| 7 | celery |
| 8 | grape |
| 9 | peach |
| 10 | melon |

$x_0$

Marked element

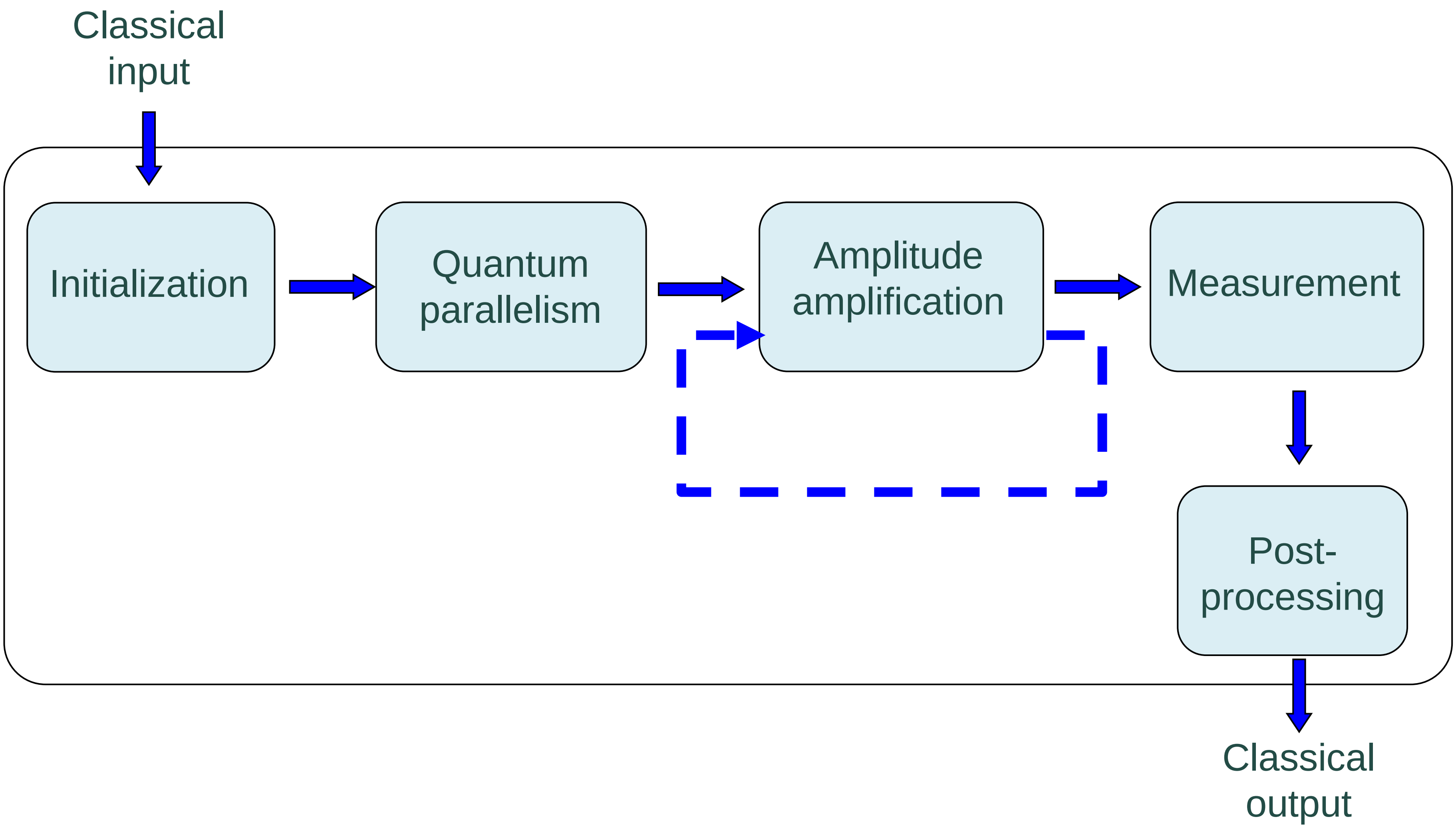
indexes

# LOV KUMAR GROVER

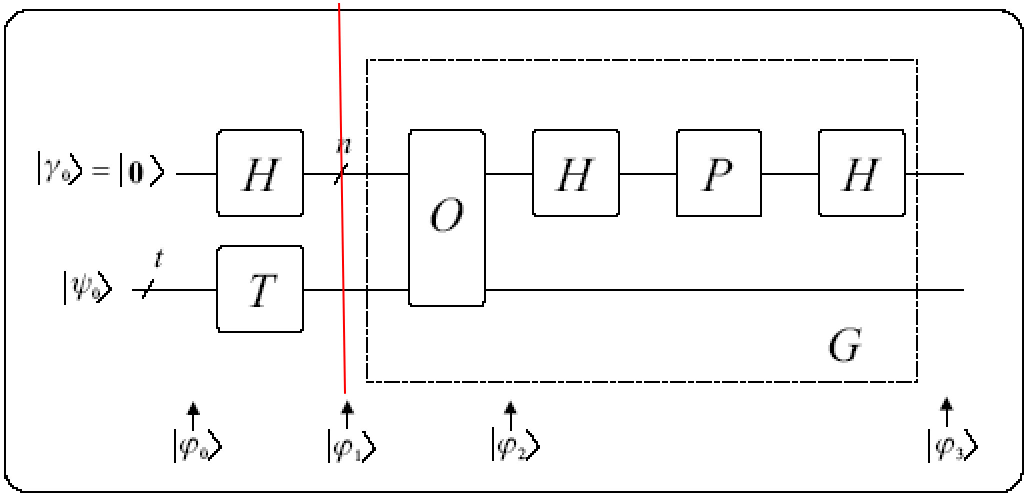


Indian-American Computer Scientist

# DESIGNING A QUANTUM ALGORITHM

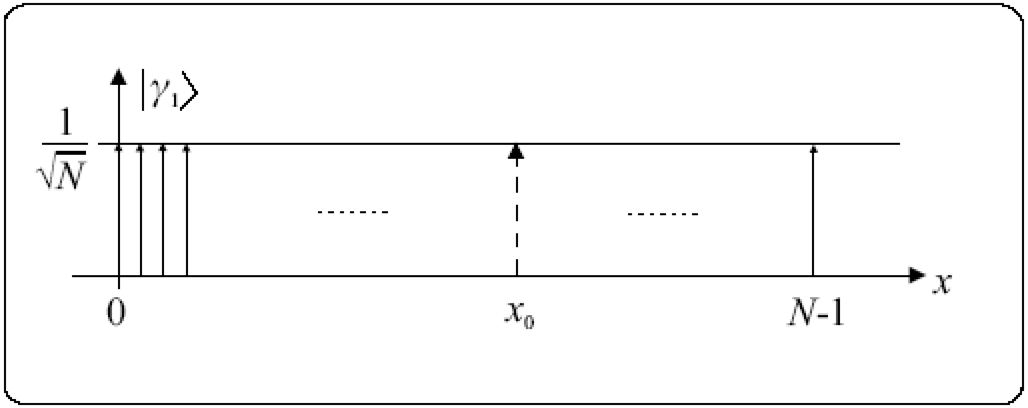


# GROVER OPERATOR – STEP 0




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

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

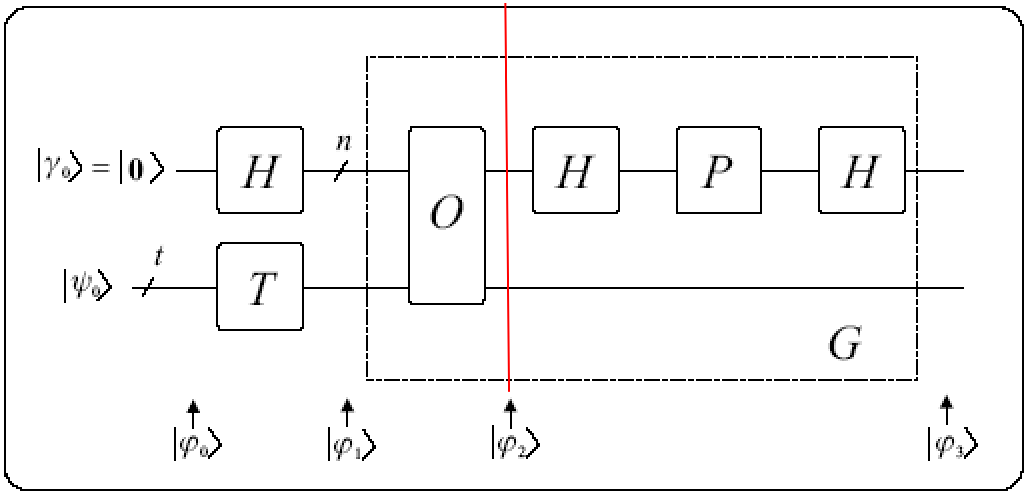


DEPARTMENT OF
NETWORKED SYSTEMS
AND SERVICES
www.hit.bme.hu

# GROVER OPERATOR – STEP 1

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

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



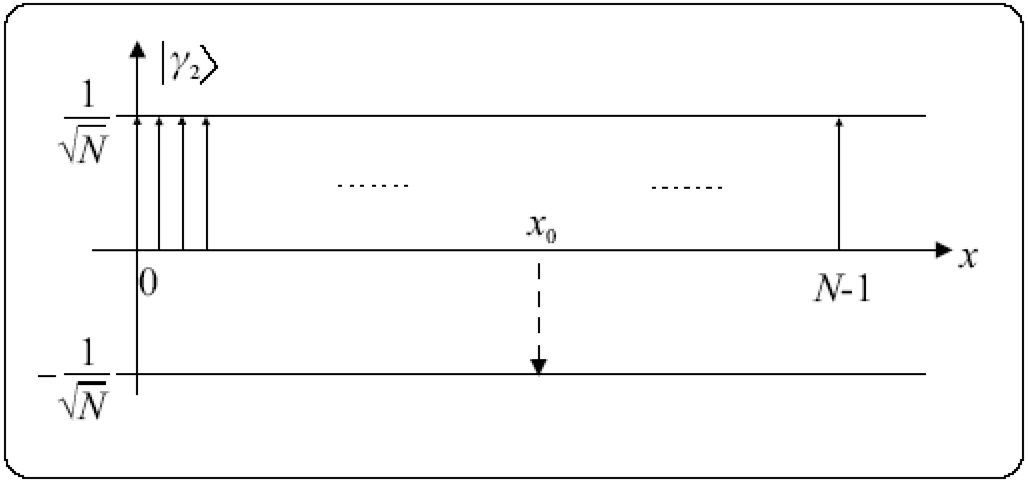

$$|\varphi_1\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

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

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

$T = H$

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



# ORACLE EXAMPLE

- 4 elements: |φ> = {|00>, |01>, |10>, |11>}

$x_0$

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

*Remember:*
|φ> = (<φ|)$^{\dagger}$

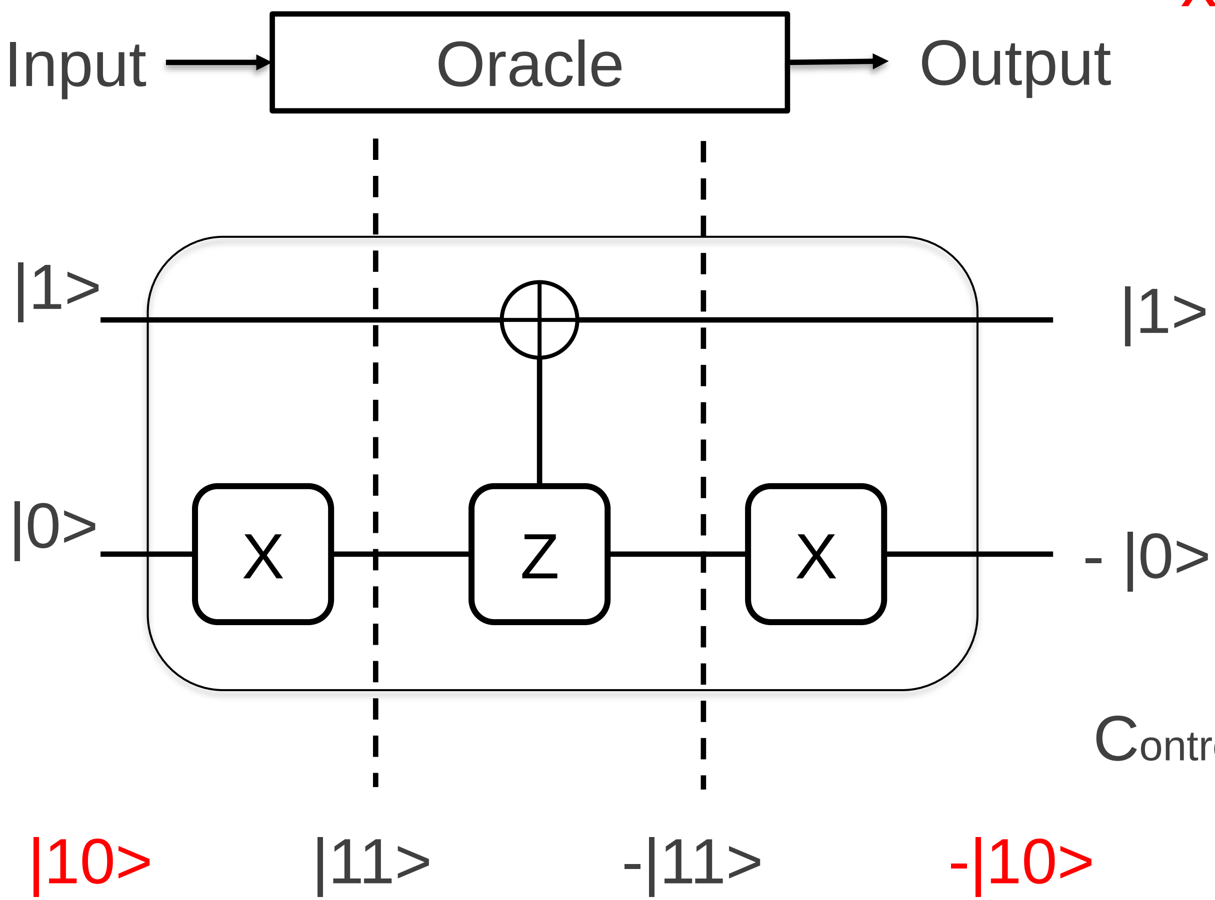
$$O = I - 2^* \left( \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \end{bmatrix} \right) = I - 2^* \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \Rightarrow O = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

# ORACLE EXAMPLE WITH GATES

- 4 elements: |φ> = {|00>, |01>, |10>, |11>}

$x_0$

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




*Remember:*

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

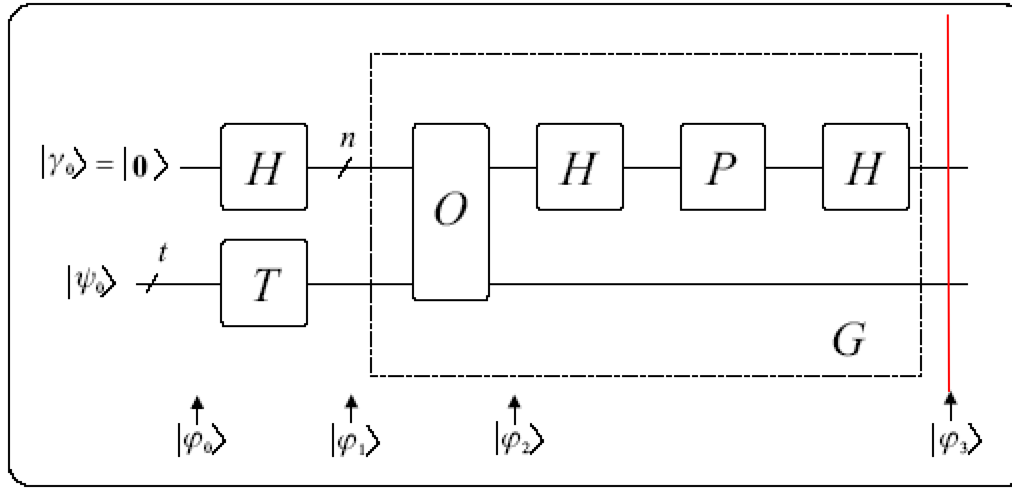
$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\text{Controlled } Z = \begin{pmatrix} 1 & 0 & & \\ 0 & 1 & & \\ & & 1 & 0 \\ & & 0 & -1 \end{pmatrix}$$

# GROVER OPERATOR – STEP 2

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

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



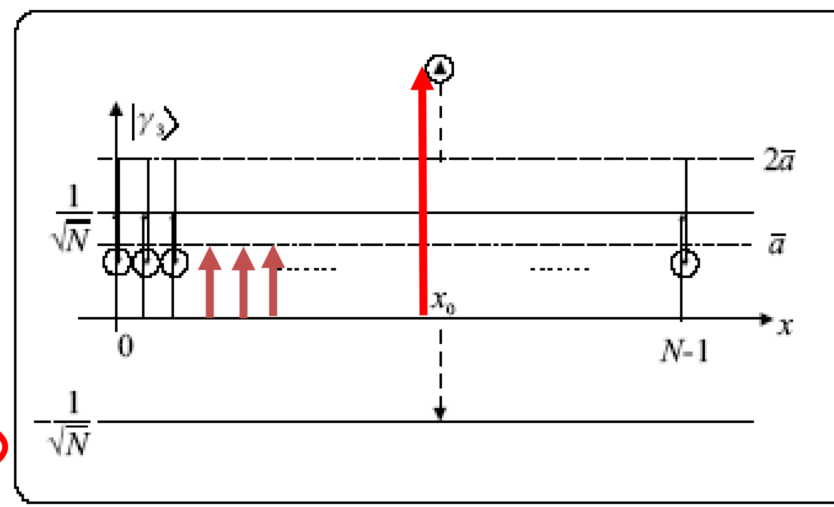

$$|\gamma_3\rangle = \sum_{x=0}^{N-1}(2\overline{a} - \gamma_{2x})|x\rangle = 2\sum_{x=0}^{N-1}\overline{a}|x\rangle - \sum_{x=0}^{N-1}\gamma_{2x}|x\rangle$$

$$\boxed{G = HPHO}$$

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

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

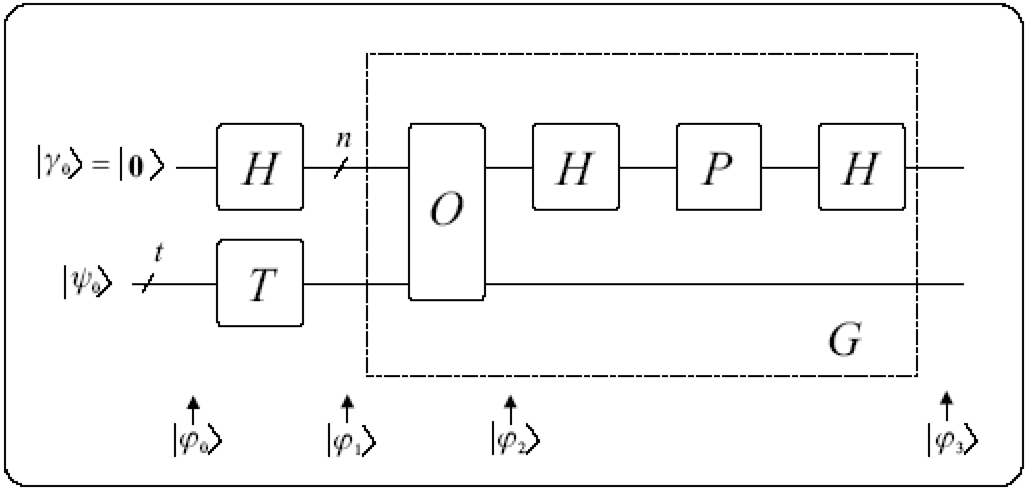
$$U_\gamma = 2|\gamma_1\rangle\langle\gamma_1| - I = H(2|\mathbf{0}\rangle\langle\mathbf{0}| - I)H$$



# GEOMETRICAL INTERPRETATION

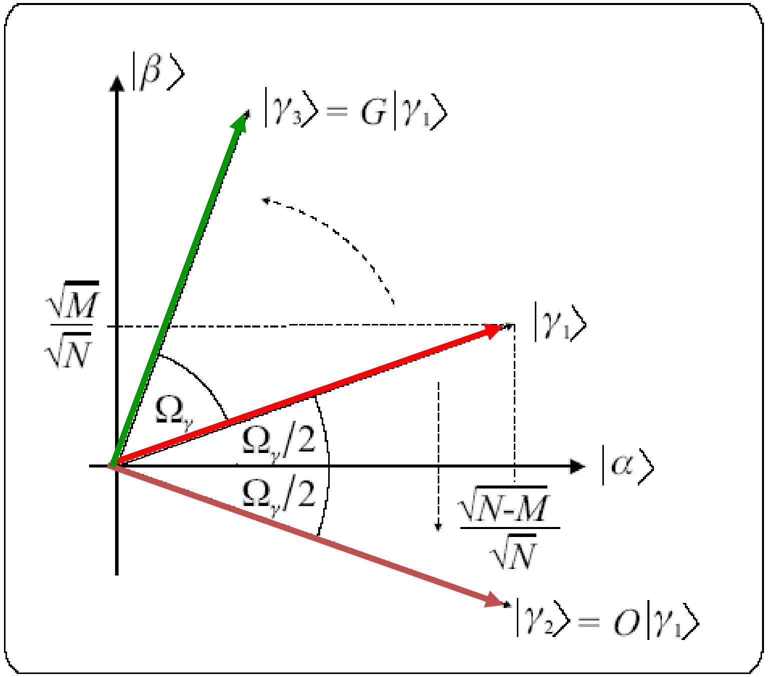
$$|\alpha\rangle \triangleq \frac{1}{\sqrt{N-M}}\sum_{x\in\overline{S}}|x\rangle,$$

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




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

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



# REQUIRED NUMBER OF ITERATIONS

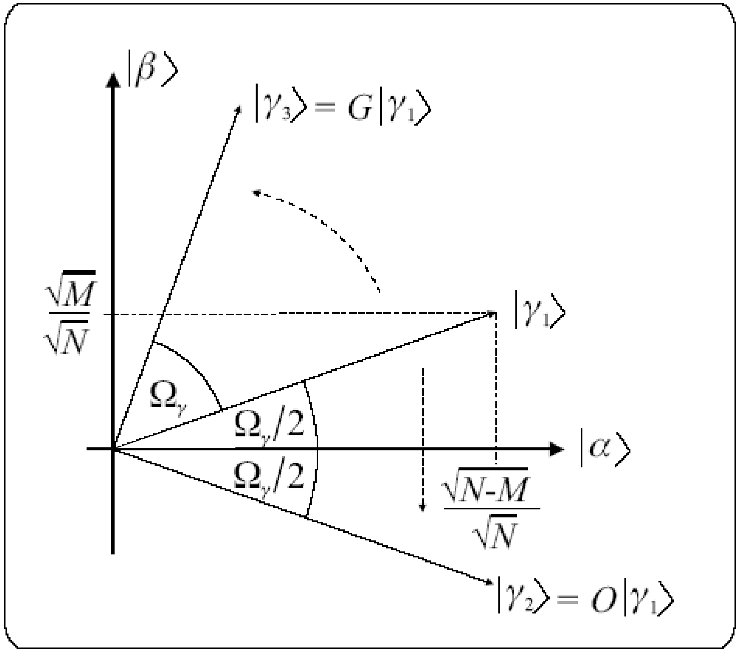
$$G^l|\gamma_1\rangle = \cos\left(l\Omega_\gamma + \frac{\Omega_\gamma}{2}\right)|\alpha\rangle + \sin\left(l\Omega_\gamma + \frac{\Omega_\gamma}{2}\right)|\beta\rangle$$

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

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

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

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

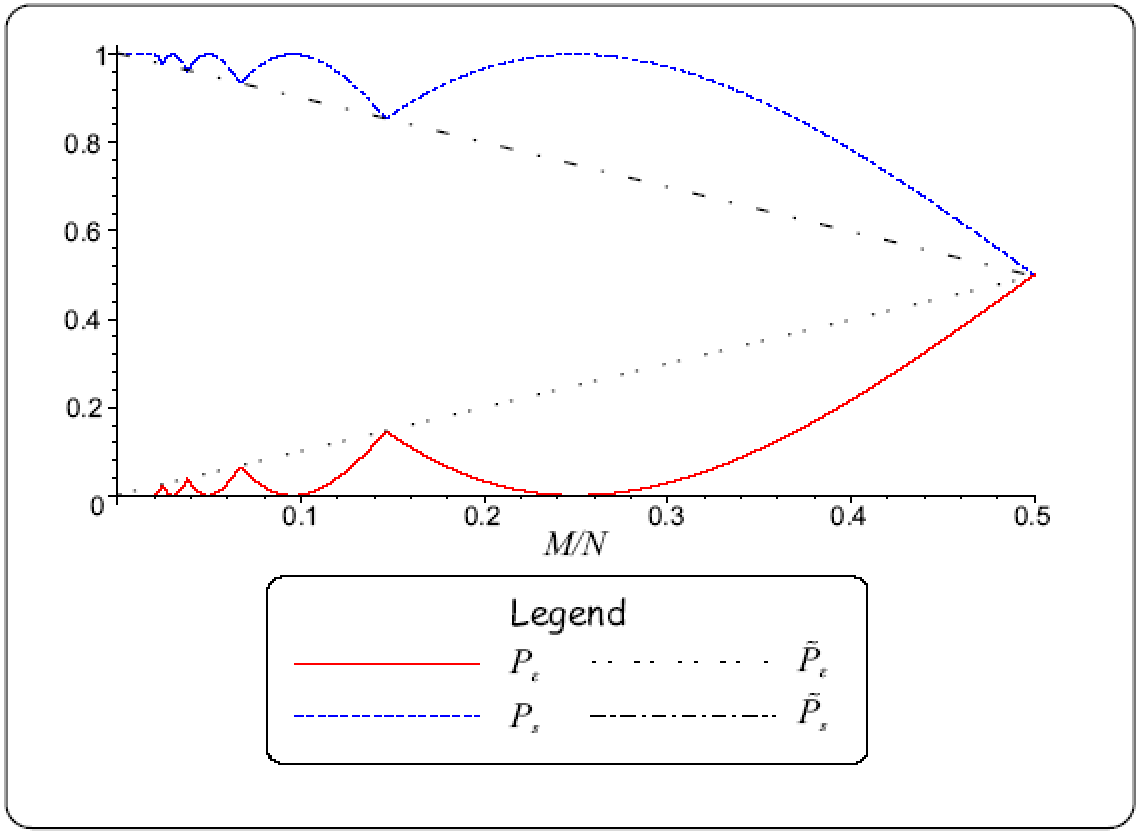


# ERROR ANALYSIS

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

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

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



# QUESTIONS

- What will happen if $M=N/2$ ?
- What shall we do if $M>N/2$ ?
- Is it possible to find the marked item with a single step?
- How to decrease the error probability?
  - Idea No. 1.
  - Idea No. 2.

- Simulation!

# QUANTUM COUNTING – SPECIAL PHASE ESTIMATION

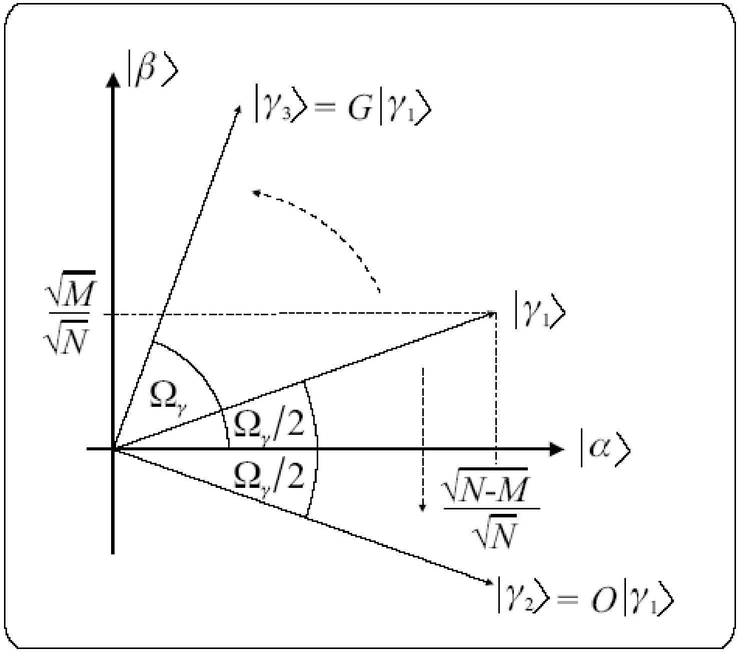
- Calculation of *M* can be traced back to phase estimation on the Grover operator.

$$\mathbf{G} = \begin{bmatrix} \cos(\Omega_\gamma) & -\sin(\Omega_\gamma) \\ \sin(\Omega_\gamma) & \cos(\Omega_\gamma) \end{bmatrix} \Rightarrow |g_1\rangle = \frac{e^{j\xi}}{\sqrt{2}}\begin{bmatrix} j \\ 1 \end{bmatrix}, |g_2\rangle = \frac{e^{j\xi}}{\sqrt{2}}\begin{bmatrix} -j \\ 1 \end{bmatrix}, \xi \in \mathbb{R}$$

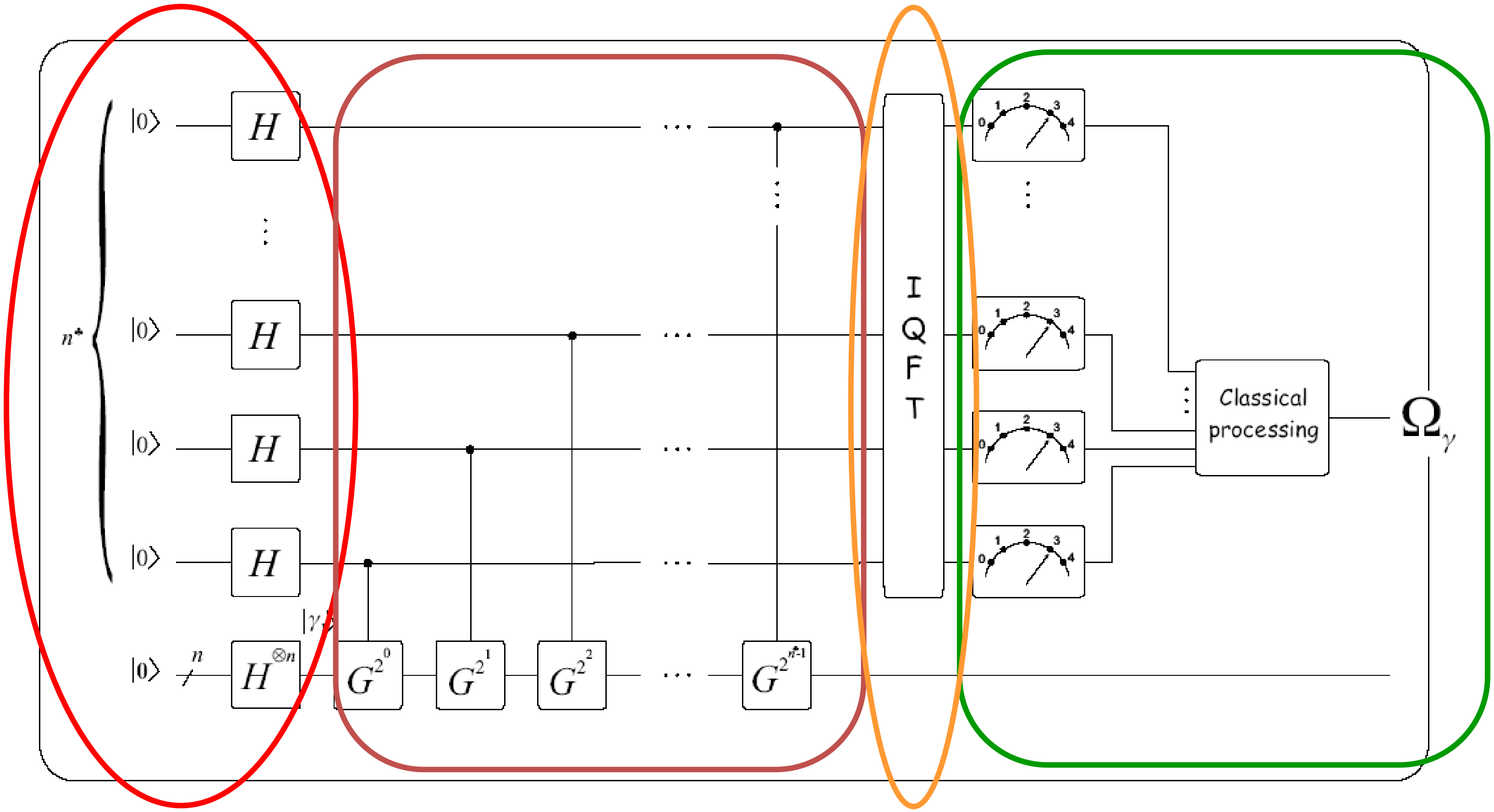
$$\Downarrow$$

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

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



# QUANTUM COUNTING – SPECIAL PHASE ESTIMATION



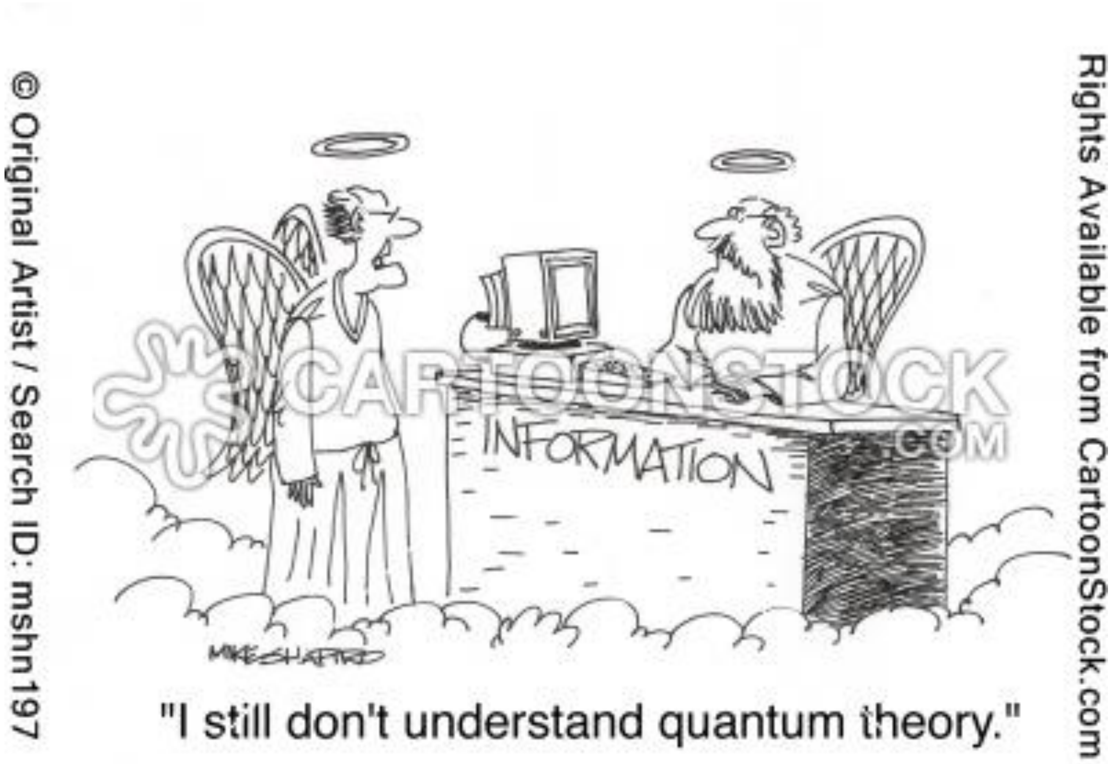

$$n^{\clubsuit} = c - 1 + \left\lceil \mathrm{ld}(2\pi) + \mathrm{ld}\left(3 + \frac{1}{\breve{P}_{\varepsilon P}}\right) \right\rceil$$

# BREAKING RSA WITH GROVER ALGORITHM

**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 $O(\mathrm{ld}(N)^3)$. ← Brutal!


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

DEPARTMENT OF
NETWORKED SYSTEMS
AND SERVICES

MŰEGYETEM 1782