Tutorial on Quantum Computing

Juris Smotrovs
University of Latvia

Eiropas Sociālā fonda projekts
“Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku”
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Outline of the tutorial

- Prehistory and history of quantum computing
- Memory
  - Qubit
  - Qubit register
- Computation: unitary operators
- Reading outcome: measurement
- Efficient quantum algorithms
  - Deutsch-Jozsa algorithm
  - Grover's algorithm

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Prehistory: quantum mechanics

- 1900: quantum hypothesis of Max Planck
- 1905: Albert Einstein's postulation of light quanta (photons)
- 1913: Niels Bohr's model of atomic structure
- 1924: Louis de Broglie's hypothesis of wave-particle duality
- 1925: Wolfgang Pauli's exclusion principle
- 1926: Erwin Schrödinger's equation
- 1926: probability density function by Max Born
- 1927: Werner Heisenberg's uncertainty principle
- 1928: Paul Dirac's equation
- 1932: mathematical foundations of QM by John von Neumann
- .....

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Prehistory: theory of computation

- 1931: Kurt Gödel's incompleteness theorems
- 1936: Emil Leon Post's machine
- 1936: undecidable problem, λ-calculus by Alonzo Church
- 1936: undecidable problem, Turing machine by Alan Turing
- 1939: Stephen Cole Kleene's recursion theory
- 1945: John von Neumann's computer architecture
- 1948: information theory by Claude E. Shannon
- 1956: Noam Chomsky's grammar hierarchy
- 1965: complexity theory, Juris Hartmanis and Richard Stearns
- 1971: Stephen Cook formulates the P = NP? problem
- .....

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

History of quantum computation

- 1973: reversible computation, Charles H. Bennett
- 1973: Alexander Holevo's bound on quantum information
- 1981: Richard Feynman's idea of a quantum computer
- 1984: quantum key distribution, Charles H. Bennett and Gilles Brassard
- 1985: universal quantum computer by David Deutsch
- 1993: Dan Simon's algorithm: exponential speed-up in an oracle problem
- 1994: Peter Shor's quantum poly-time factoring algorithm
- 1996: Lov Grover's quadratic speed-up database search
- 1998: first small quantum computers
- .....

ESF
EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Basic idea

- Computation must be performed as a real, physical process, therefore it must obey physical laws
- At the fundamental level the physics are described by quantum mechanics
- Does quantum mechanics imply any differences to the (classical) computation as we know it? – YES!

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Memory: a classical bit

- Is either 0 or 1
- A one-bit-memory in the classical sense is a (classical-physics) system with two possible distinguishable states designated by 0 and 1

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Memory: a quantum bit (qubit)

- A two-state quantum system
- Its two distinguishable states are designated by $|0\rangle$ and $|1\rangle$

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Quantum principle No. 1

- Quantum principle of superposition: if a quantum system can be in any of n distinguishable (basis) states, then it can also be in any superposition of these states, with complex numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$, called (probability) amplitudes, characterizing the amount by which the system is in respective basis states. It must hold:

$$|\alpha_1|^2 + |\alpha_2|^2 + \ldots + |\alpha_n|^2 = 1$$

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Memory: a quantum bit (qubit)

- Thus qubit can be also in any superposition of $|0\rangle$ and $|1\rangle$, with some amplitudes α_0 and α_1
- Such superposition state is denoted:

$$\alpha_0 |0\rangle + \alpha_1 |1\rangle$$

- α_0 and α_1 are complex numbers with

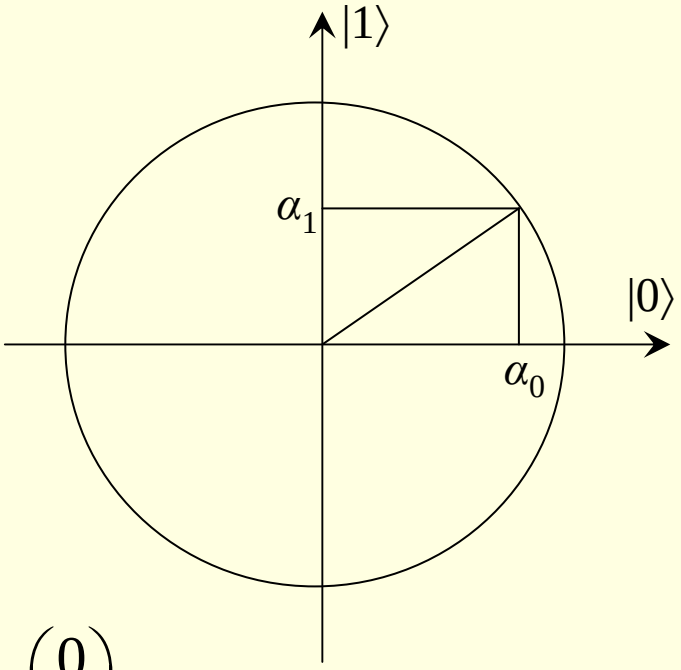
$$|\alpha_0|^2 + |\alpha_1|^2 = 1$$

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Memory: a quantum bit (qubit)

- The state of a qubit can also be described by a vector in $\mathbb{C}^2$: $\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$
- Thus $|0\rangle = 1\,|0\rangle + 0\,|1\rangle$ or $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$
- ... and $|1\rangle = 0\,|0\rangle + 1\,|1\rangle$ or $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$



ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Memory: a quantum bit (qubit)

- The exact state of an unknown qubit $\alpha_0 |0\rangle + \alpha_1 |1\rangle$ cannot be learned
- The information from a qubit can be obtained by a measurement (we will talk about it in more detail later)
- One can measure whether qubit is in state $|0\rangle$ or $|1\rangle$
- Then one will obtain:
  - the answer $|0\rangle$ with probability $|\alpha_0|^2$,
  - the answer $|1\rangle$ with probability $|\alpha_1|^2$
- After the measurement the qubit collapses to the state equal with the given answer

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Memory: a qubit register

- We can put 2 qubits $\alpha_0 |0\rangle + \alpha_1 |1\rangle$ and $\beta_0 |0\rangle + \beta_1 |1\rangle$ together forming a two qubit register
- Then if we measure both qubits, we will obtain for the first qubit:
  - the answer $|0\rangle$ with probability $|\alpha_0|^2$,
  - the answer $|1\rangle$ with probability $|\alpha_1|^2$
- ... and for the second qubit:
  - the answer $|0\rangle$ with probability $|\beta_0|^2$,
  - the answer $|1\rangle$ with probability $|\beta_1|^2$

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Memory: a qubit register

- Alternatively, we can look on a two qubit register as on a four state $|0\rangle|0\rangle$, $|0\rangle|1\rangle$, $|1\rangle|0\rangle$, $|1\rangle|1\rangle$ system
- From such viewpoint we will get:
  - the answer $|0\rangle|0\rangle$ with probability $|\alpha_0\beta_0|^2$,
  - the answer $|0\rangle|1\rangle$ with probability $|\alpha_0\beta_1|^2$,
  - the answer $|1\rangle|0\rangle$ with probability $|\alpha_1\beta_0|^2$,
  - the answer $|1\rangle|1\rangle$ with probability $|\alpha_1\beta_1|^2$

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Memory: a qubit register

- A multiplication law works:

$$\left(\alpha_0|0\rangle+\alpha_1|1\rangle\right)\otimes\left(\beta_0|0\rangle+\beta_1|1\rangle\right)=$$
$$\alpha_0\beta_0|0\rangle\otimes|0\rangle+\alpha_0\beta_1|0\rangle\otimes|1\rangle+\alpha_1\beta_0|1\rangle\otimes|0\rangle+\alpha_1\beta_1|1\rangle\otimes|1\rangle$$

- $|0\rangle \otimes |0\rangle$ denotes the same as $|0\rangle\ |0\rangle$ or $|00\rangle$
- This multiplication is called tensor multiplication
- It is not commutative:
  $|0\rangle \otimes |1\rangle$ is not the same as $|1\rangle \otimes |0\rangle$

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Memory: a qubit register

- A tensor or Kronecker product of matrices:

$$A = (a_{ij}) \text{ of size } m \times n,\ B = (b_{ij}) \text{ of size } k \times l$$

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \dots & \dots & \dots & \dots \\ a_{m1}B & a_{m2}B & \dots & a_{mn}B \end{pmatrix} \text{ of size } mk \times nl$$

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Memory: a qubit register

- For our two qubits in matrix form:

$$\begin{pmatrix}\alpha_0\\ \alpha_1\end{pmatrix}\otimes\begin{pmatrix}\beta_0\\ \beta_1\end{pmatrix}=\begin{pmatrix}\alpha_0\begin{pmatrix}\beta_0\\ \beta_1\end{pmatrix}\\ \alpha_1\begin{pmatrix}\beta_0\\ \beta_1\end{pmatrix}\end{pmatrix}=\begin{pmatrix}\alpha_0\beta_0\\ \alpha_0\beta_1\\ \alpha_1\beta_0\\ \alpha_1\beta_1\end{pmatrix}$$

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Quantum principle No. 1

- Quantum principle of superposition: if a quantum system can be in any of n distinguishable (basis) states, then it can also be in any superposition of these states, with complex numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$, called (probability) amplitudes, characterizing the amount by which the system is in respective basis states. It must hold:

$$|\alpha_1|^2 + |\alpha_2|^2 + \ldots + |\alpha_n|^2 = 1$$

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Memory: a qubit register

- General state of a two qubit register:

$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

$$\text{where } |\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Memory: a qubit register

- There are such states that cannot be expressed as a tensor product of two 1-qubit states
- It means that the 2-qubit register cannot be looked at as a composition of two independent qubits
- Such states are called entangled states

ESF
EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Memory: a qubit register

- Example, the Bell state: $\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left|00\right\rangle + \frac{1}{\sqrt{2}}\left|11\right\rangle$
- The 1st qubit:
  - is $\left|0\right\rangle$ with prob. $1/2$,
  - is $\left|1\right\rangle$ with prob. $1/2$
- The 2nd qubit:
  - is $\left|0\right\rangle$ with prob. $1/2$,
  - is $\left|1\right\rangle$ with prob. $1/2$
- ... but the register:
  - is $\left|00\right\rangle$ with prob. $1/2$,
  - is $\left|01\right\rangle$ with prob. 0,
  - is $\left|10\right\rangle$ with prob. 0,
  - is $\left|11\right\rangle$ with prob. $1/2$
- The multiplication law does not work!

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Memory: a qubit register

- General state of an *n* qubit register:

$$\alpha_{0\ldots00}\left|0\ldots00\right\rangle+\alpha_{0\ldots01}\left|0\ldots01\right\rangle+\ldots+\alpha_{1\ldots11}\left|1\ldots11\right\rangle$$

$$\text{where}\left|\alpha_{0\ldots00}\right|^2+\left|\alpha_{0\ldots01}\right|^2+\ldots+\left|\alpha_{1\ldots11}\right|^2=1$$

- Geometrically: an arbitrary vector of unit length in $\mathbb{C}^{2^n}$

$$\begin{pmatrix}\alpha_{0\ldots00}\\ \alpha_{0\ldots01}\\ \ldots\\ \alpha_{1\ldots11}\end{pmatrix}$$

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Quantum principle No. 2

- Quantum principle of state evolution: the change of the state of a quantum system is a unitary linear operator
- A linear operator is unitary iff it preserves the vector norm
- ... alternatively, it maps the unit hypersphere (where the quantum state vectors reside) to itself
- Essentially, unitary operators are the rotations
- Since unitary operators are linear, to define them it is enough to specify their action on the basis vectors

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Computation: unitary operators

- 1-qubit unitary operator examples:

$$\text{identity operator}: \quad id = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\text{NOT operator}: \quad NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\text{rotation}: \quad R_{\varphi} = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$$

$$\text{phase shift}: \quad P_{\varphi} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$$

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Computation: unitary operators

- 1-qubit unitary operator example, the Hadamard transform:

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

$$|1\rangle \rightarrow \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

$$H = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}$$

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Computation: unitary operators

- 2-qubit unitary operator example, the controlled NOT operator:

$$|00\rangle \rightarrow |00\rangle$$
$$|01\rangle \rightarrow |01\rangle$$
$$|10\rangle \rightarrow |11\rangle$$
$$|11\rangle \rightarrow |10\rangle$$

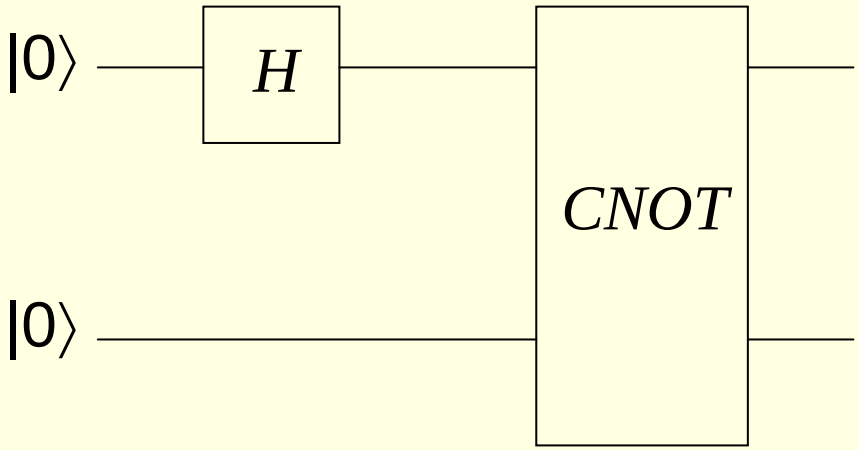
$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Computation: unitary operators

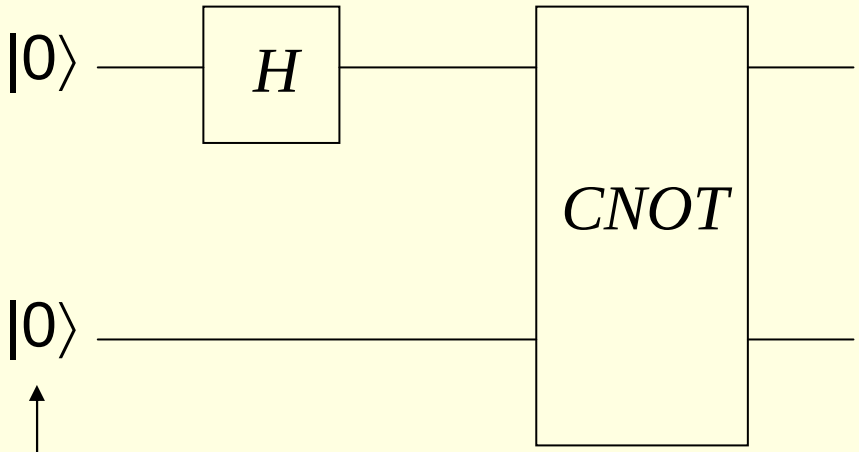
- Example of a computation, creation of the Bell state $|\Phi^+\rangle$:



Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Computation: unitary operators

- Example of a computation, creation of the Bell state $|\Phi^+\rangle$:

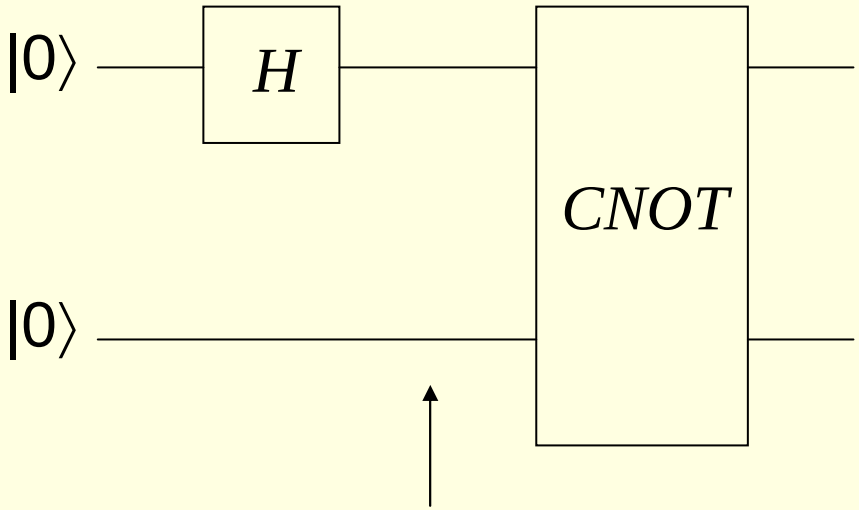


$$|0\rangle \otimes |0\rangle = |00\rangle$$

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Computation: unitary operators

- Example of a computation, creation of the Bell state $|\Phi^+\rangle$:

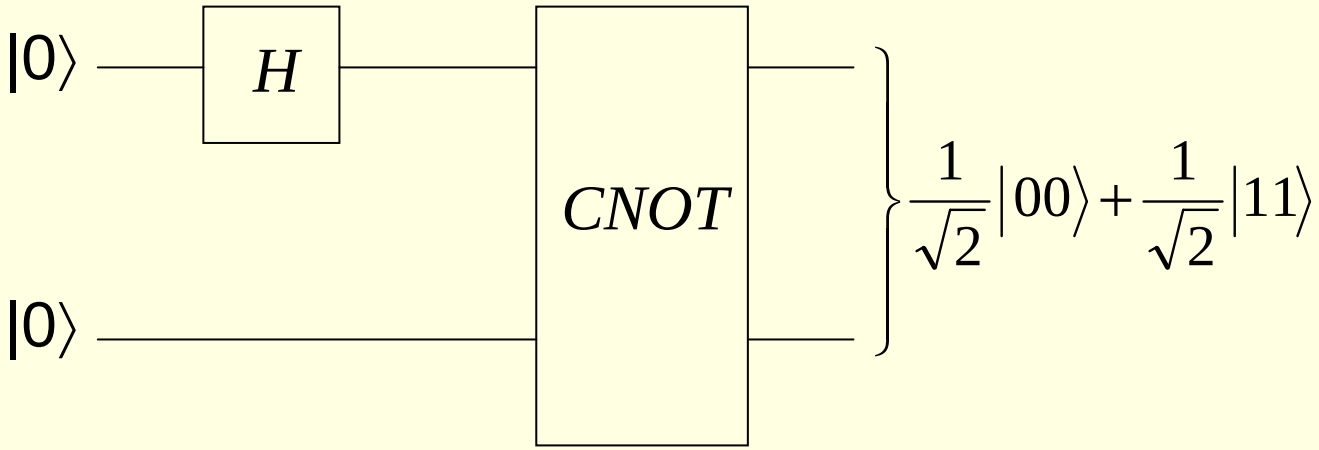


$$\left(\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle\right)\otimes|0\rangle=\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|10\rangle$$

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Computation: unitary operators

- Example of a computation, creation of the Bell state $|\Phi^+\rangle$:



Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Quantum principle No. 3

- Any information about the state of a quantum system can be extracted into the macroscopic world only by means of a measurement
- Mathematically measurement means partitioning the state space H into orthogonal subspaces: $H = E_1 \oplus E_2 \oplus \ldots \oplus E_k$
- If the state vector before measurement is $|\psi\rangle = \sum_{i=1}^{k} |proj_{E_i}\psi\rangle$
- ... then after the measurement the state collapses randomly, with probability $||proj_{Ei}\,\psi||^2$ to one of the subspaces:

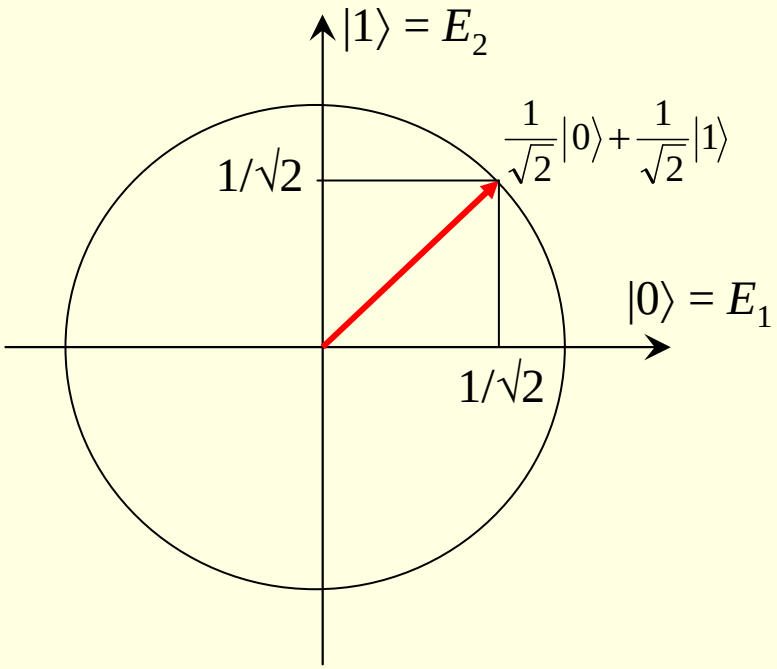
$$|\psi\rangle \rightarrow |proj_{E_i}\psi\rangle / \|proj_{E_i}\psi\|$$

- The only classical information obtained is i

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Reading outcome: measurement

- Example of a measurement:

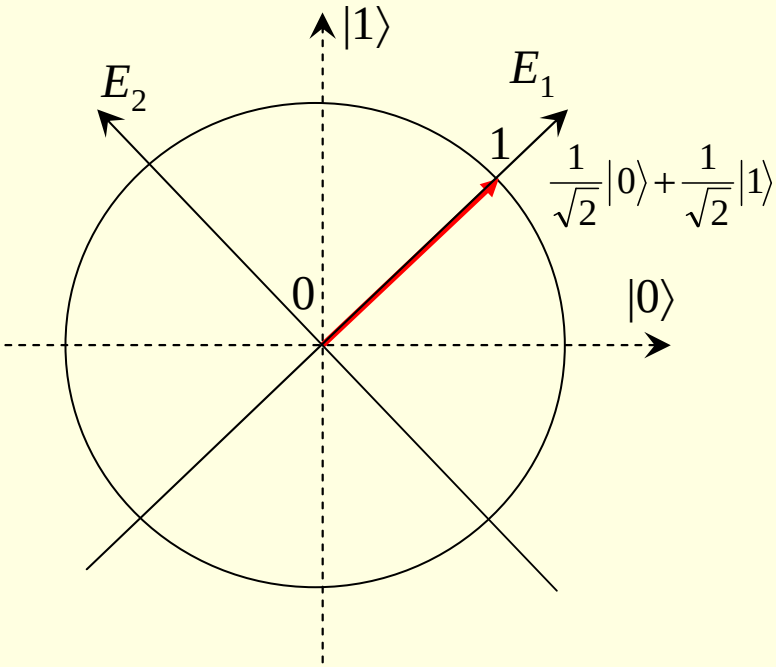


- Outcome E_1 with probability ½
- Outcome E_2 with probability ½

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Reading outcome: measurement

- Example of a measurement:



- Outcome E_1 with probability 1
- Outcome E_2 with probability 0

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Reading outcome: measurement

- Example: measuring only the first qubit of a 2-qubit system

$$|\psi\rangle = 1/\sqrt{2}|00\rangle + 1/\sqrt{2}|11\rangle$$

$$E_1 = span(|00\rangle, |01\rangle)$$

$$E_2 = span(|10\rangle, |11\rangle)$$

Outcome E_1 with probability $1/2$

Outcome E_2 with probability $1/2$

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Reading outcome: measurement

- Example: measuring only the first qubit of a 2-qubit system

$$|\psi\rangle = 1/\sqrt{2}|00\rangle + 1/\sqrt{2}|11\rangle$$

$$E_1 = span\left(\left(1/\sqrt{2}|0\rangle + 1/\sqrt{2}|1\rangle\right)\otimes|0\rangle, \left(1/\sqrt{2}|0\rangle + 1/\sqrt{2}|1\rangle\right)\otimes|1\rangle\right)$$

$$E_2 = span\left(\left(1/\sqrt{2}|0\rangle - 1/\sqrt{2}|1\rangle\right)\otimes|0\rangle, \left(1/\sqrt{2}|0\rangle - 1/\sqrt{2}|1\rangle\right)\otimes|1\rangle\right)$$

Outcome E_1 with probability $1/2$

Outcome E_2 with probability $1/2$

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Efficient quantum algorithm

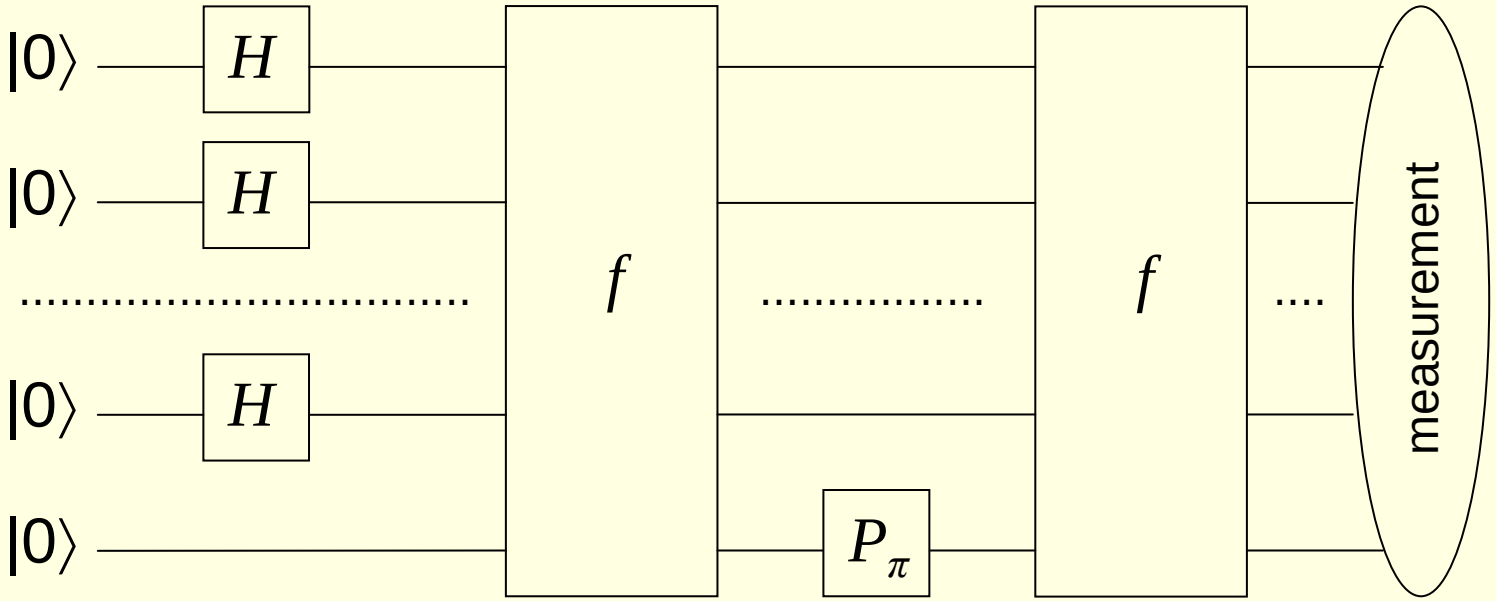
- Example: the Deutsch-Jozsa algorithm (1992)
- Input: a black-box function f: $\{0,1\}^n \rightarrow \{0,1\}$ which is
  - either constant (i.e. all its values are equal),
  - or balanced (i.e. half of its values are 0, and the other half are 1)
- The algorithm can query the black box; the number of queries determines the complexity of algorithm
- The black box works like this: input $|x\rangle|b\rangle$, output $|x\rangle|b \oplus f(x)\rangle$
- Output: answer “constant” or “balanced”

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
“Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku”
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Efficient quantum algorithm

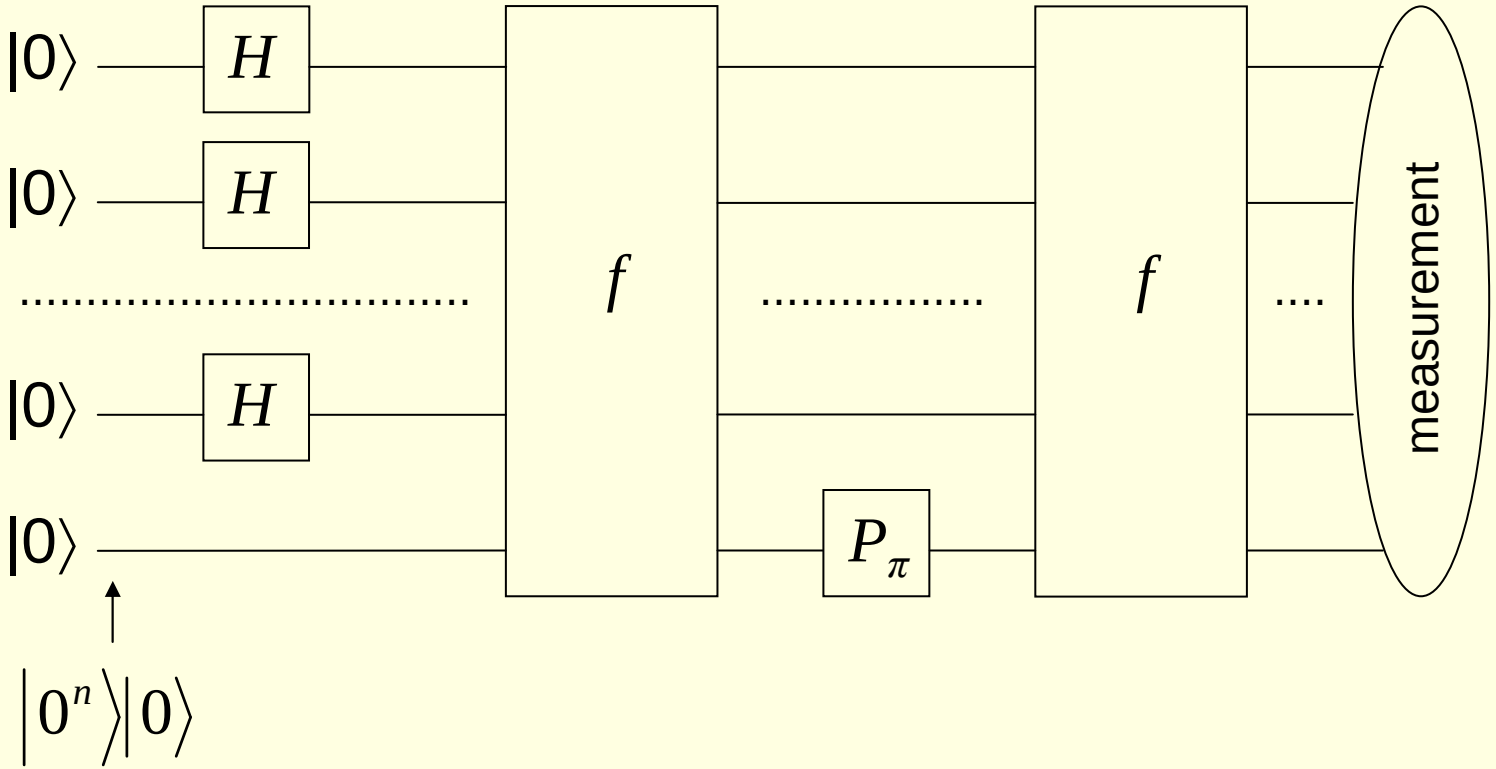
- Example: the Deutsch-Jozsa algorithm (1992)



Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Efficient quantum algorithm

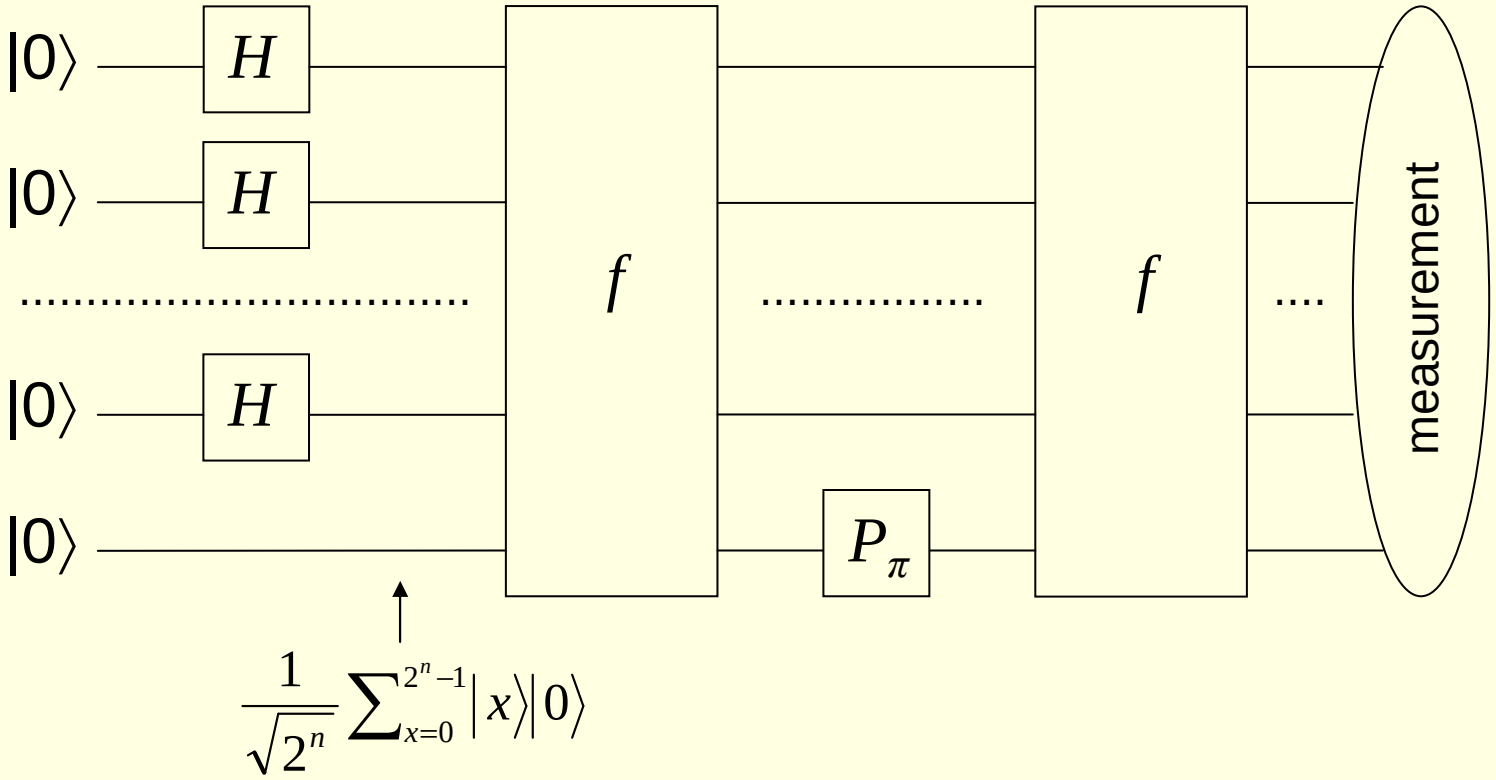
- Example: the Deutsch-Jozsa algorithm (1992)



Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Efficient quantum algorithm

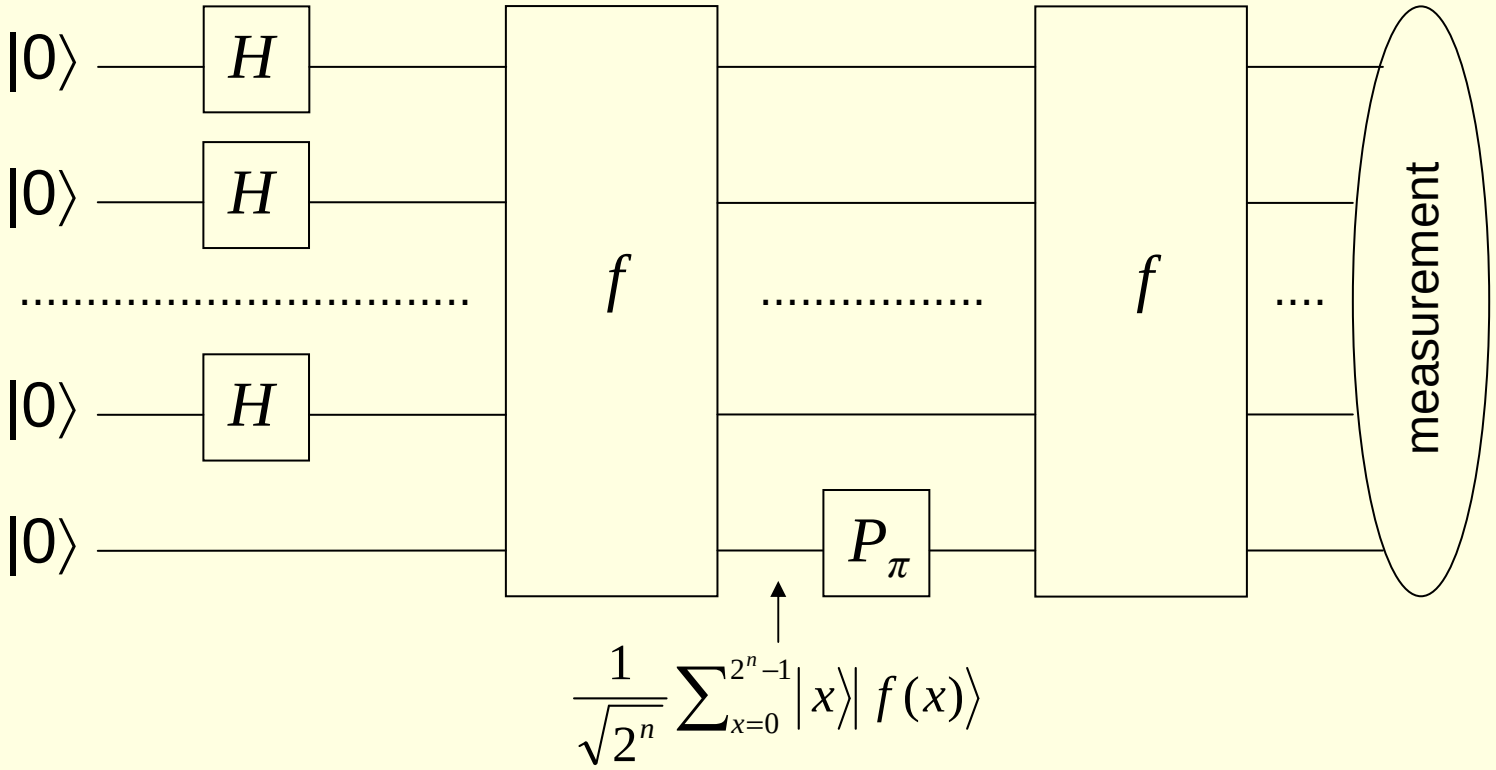
- Example: the Deutsch-Jozsa algorithm (1992)



Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Efficient quantum algorithm

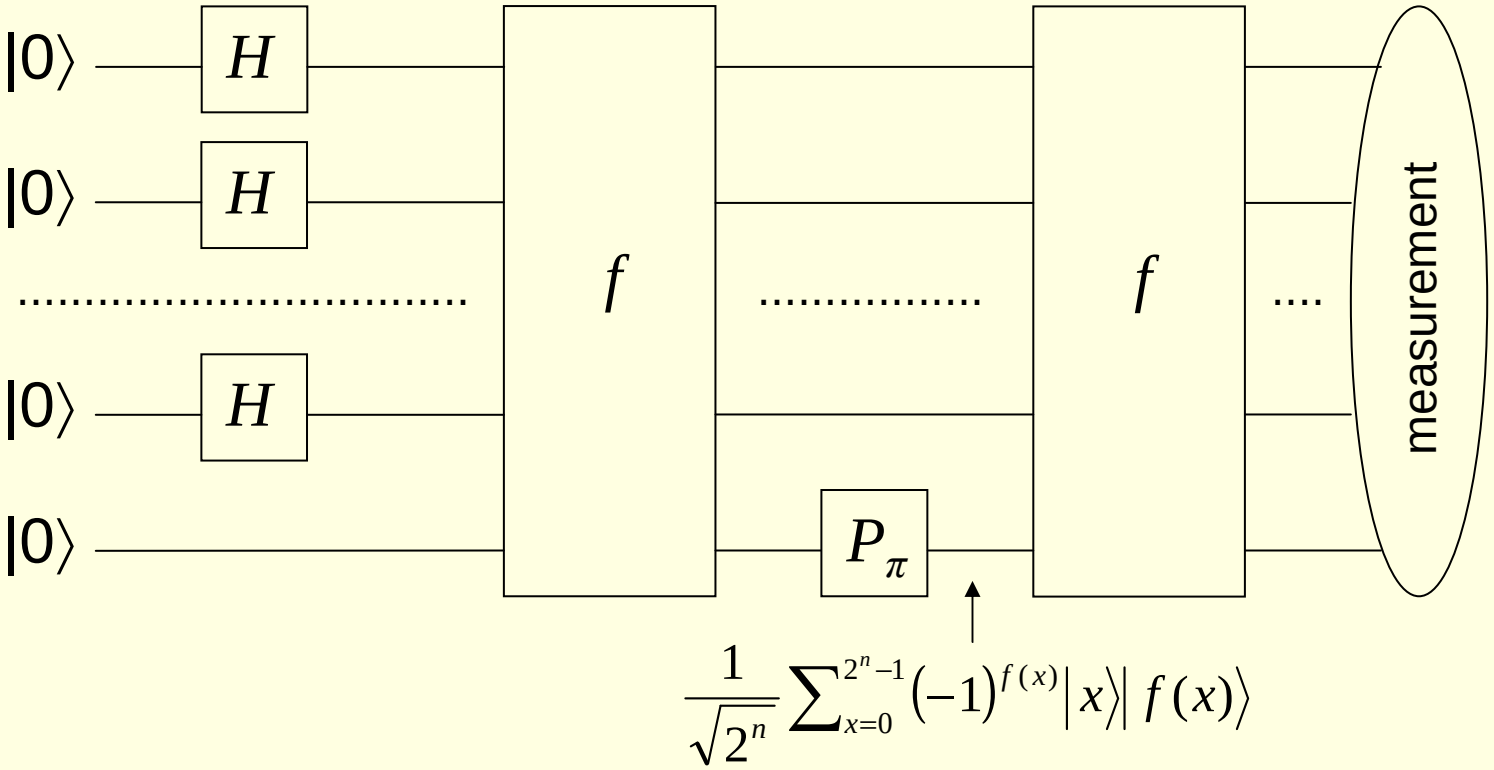
- Example: the Deutsch-Jozsa algorithm (1992)



Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Efficient quantum algorithm

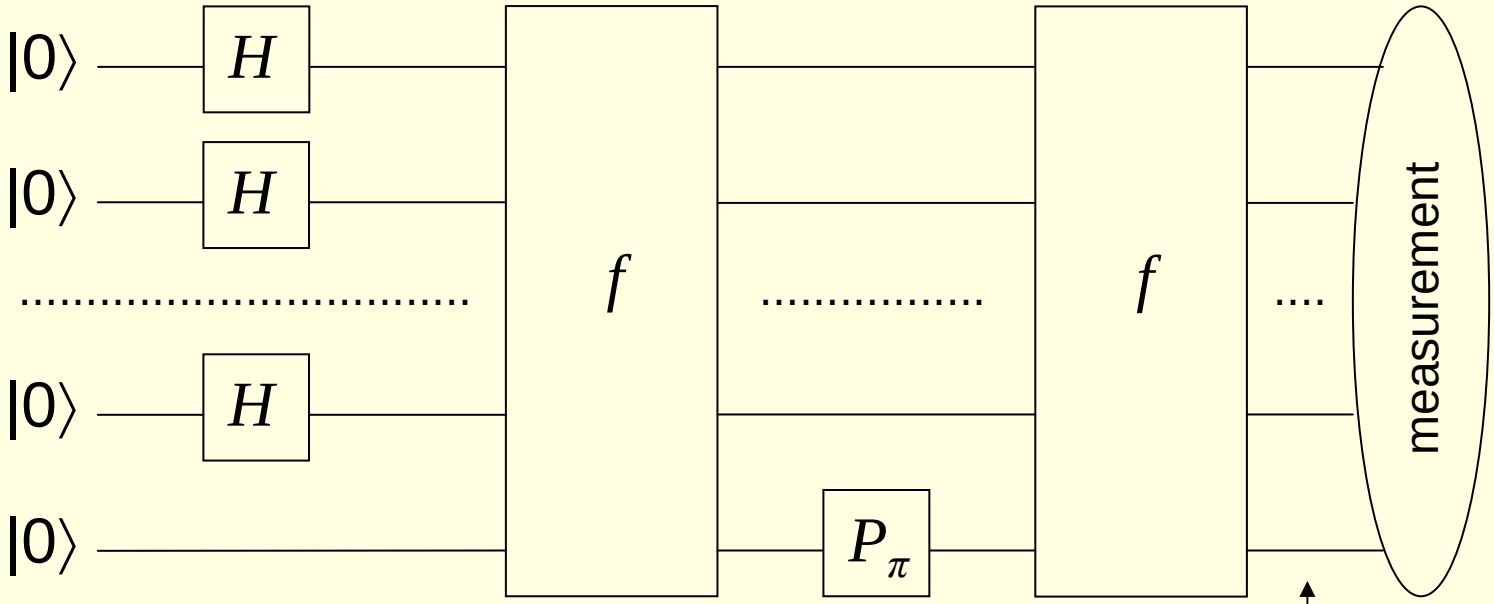
- Example: the Deutsch-Jozsa algorithm (1992)



Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Efficient quantum algorithm

- Example: the Deutsch-Jozsa algorithm (1992)

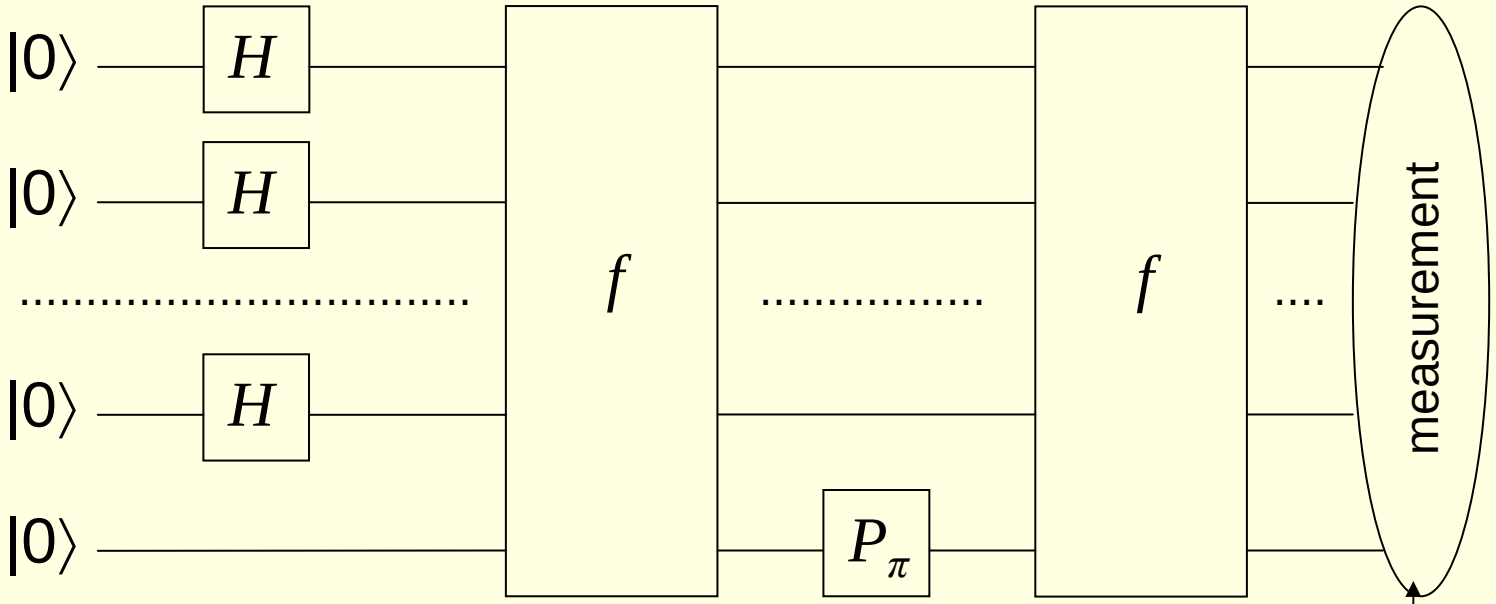


ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Efficient quantum algorithm

- Example: the Deutsch-Jozsa algorithm (1992)



$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle |0\rangle, \quad E_{\text{constant}} = span\left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |0\rangle \right), \quad E_{\text{balanced}} = E_{\text{constant}}^{\perp}$$

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Efficient quantum algorithm

- E_{constant} is one-dimensional: $E_{\text{constant}} = span(|\theta\rangle)$ where

$$\theta = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|0\rangle$$

- Therefore the length of the projection of $|\psi\rangle$ on E_{constant} is the scalar product of $|\psi\rangle$ and $|\theta\rangle$, denoted by $\langle\psi|\theta\rangle$:

$$\langle\psi|\theta\rangle = \sum_{x=0}^{2^n-1} \frac{1}{\sqrt{2^n}} \cdot (-1)^{f(x)} \cdot \frac{1}{\sqrt{2^n}} = \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)}$$

- ... which is by absolute value 1 iff f is constant, and 0 iff f is balanced
- The quantum algorithm is correct with probability 1 and with just two queries (classically $2^{n-1}+1$ are needed in the worst case)

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Efficient quantum algorithm

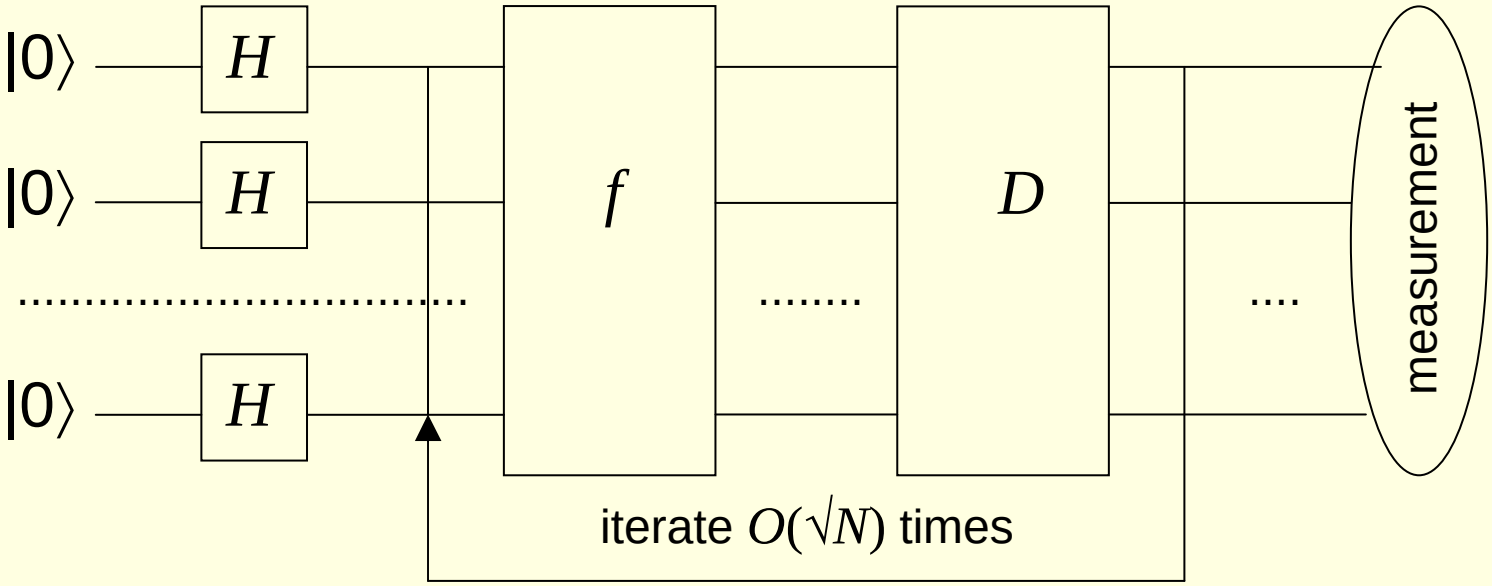
- Another example: Grover's algorithm (1996)
- Input: a black-box function f: $\{0,1\}^n \longrightarrow \{0,1\}$ such that $f(x) = 1$ just for one (unknown) value, $x = x_0$; for all other values $f(x) = 0$
- The algorithm can query the black box; the number of queries determines the complexity of algorithm
- The black box queries on classical inputs work like this: input $|x\rangle$, output $(-1)^{f(x)}|x\rangle$
- Output: x_0

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Efficient quantum algorithm

- Example: the Grover's algorithm (1996)



$$N = 2^n$$

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Efficient quantum algorithm

- The matrix of the f-query transformation

$$f\text{-query} = \begin{pmatrix} 1 & \dots & 0 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 1 & 0 & 0 & \dots & 0 \\ 0 & \dots & 0 & -1 & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

$$|x_0\rangle$$

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Efficient quantum algorithm

- The matrix of the D (diffusion) transformation

$$D = \begin{pmatrix} \frac{2}{N}-1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N}-1 & \cdots & \frac{2}{N} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N}-1 \end{pmatrix} = \frac{2}{N} J - I$$

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Efficient quantum algorithm

- D performs on the vector components inversion about their arithmetic mean

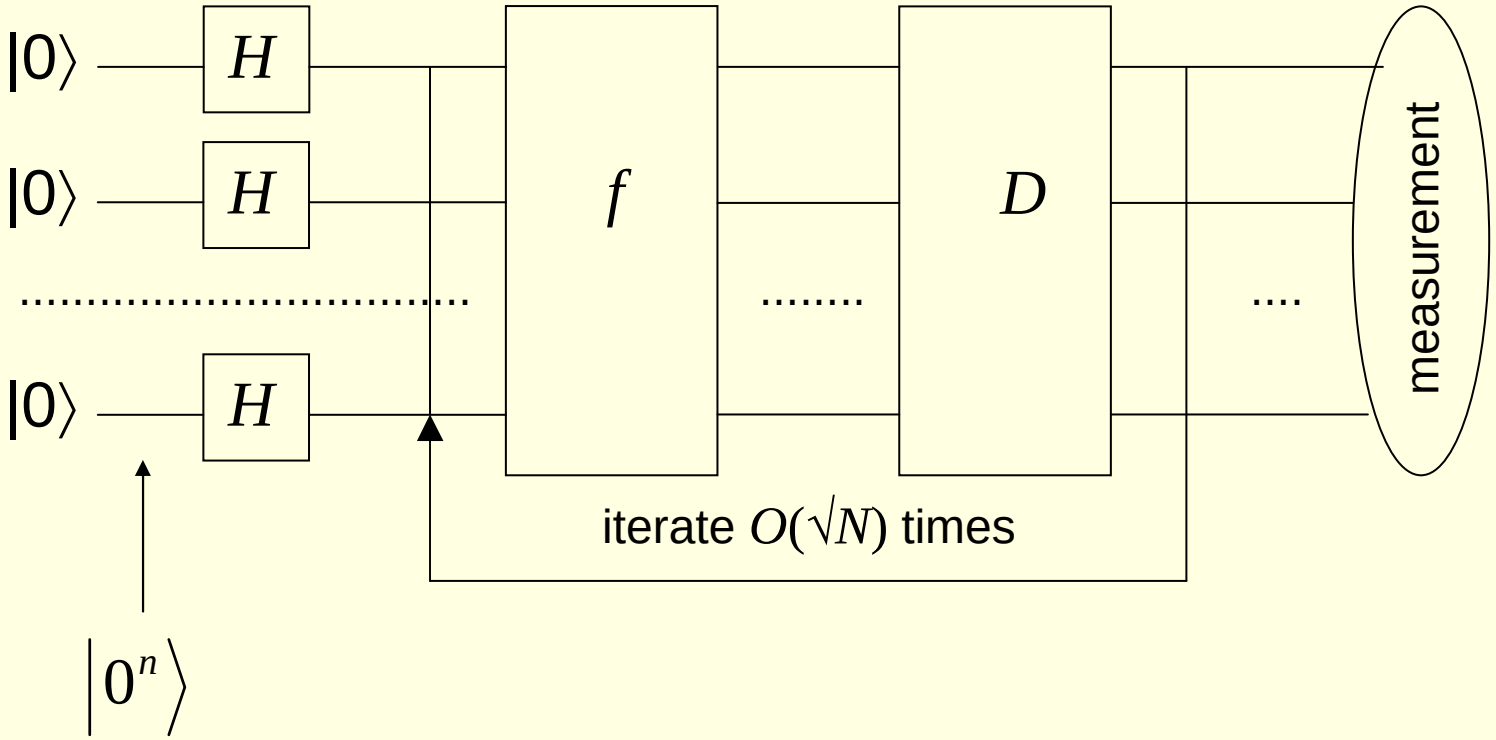
$$D \cdot \begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_N \end{pmatrix} = \left(\tfrac{2}{N} J - I\right) \cdot \begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_N \end{pmatrix} = \begin{pmatrix} 2m - a_1 \\ 2m - a_2 \\ \dots \\ 2m - a_N \end{pmatrix} = \begin{pmatrix} m + (m - a_1) \\ m + (m - a_2) \\ \dots \\ m + (m - a_N) \end{pmatrix}$$

where $\quad m = \dfrac{a_1 + a_2 + \ldots + a_N}{N}$

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Efficient quantum algorithm

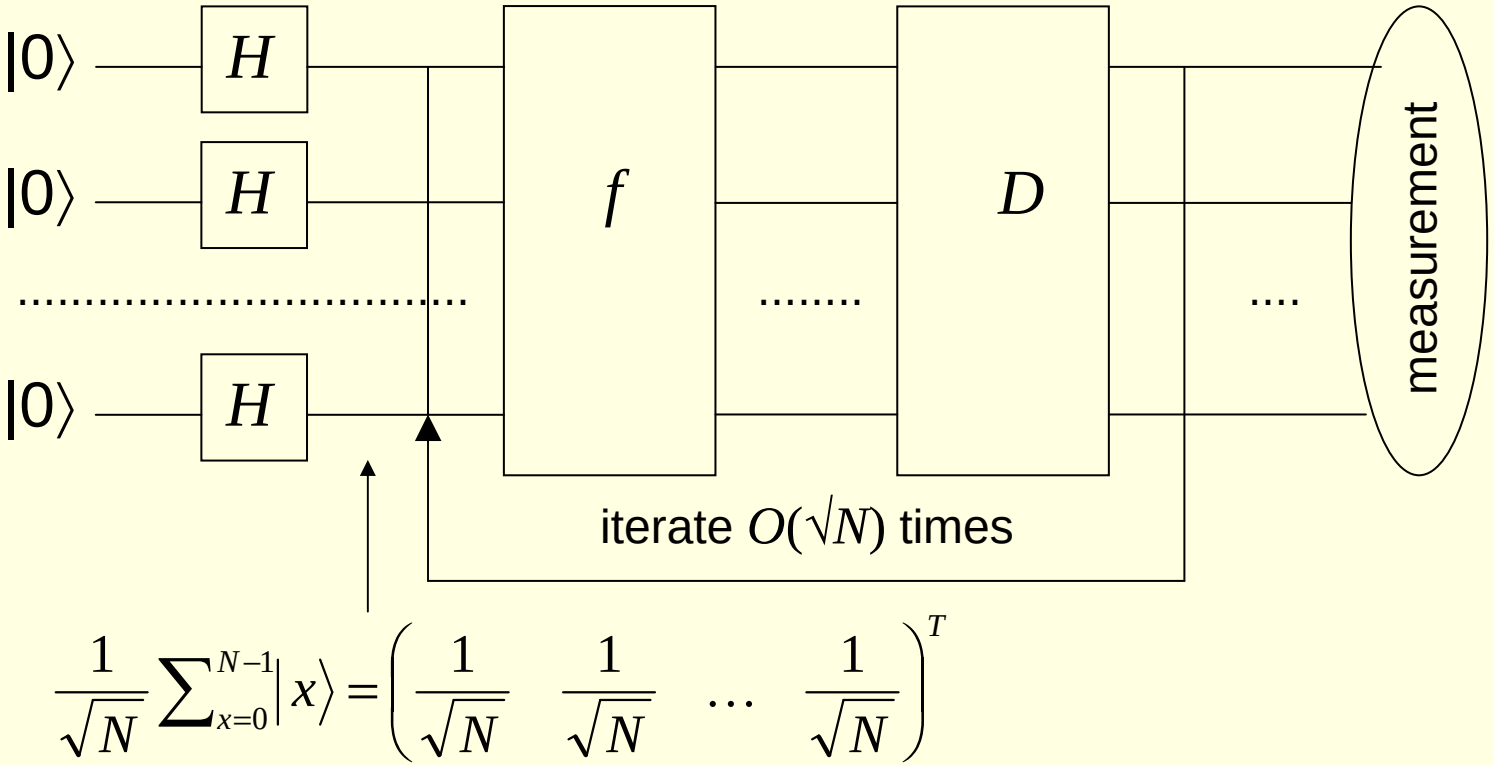
- Example: the Grover's algorithm (1996)



Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Efficient quantum algorithm

- Example: the Grover's algorithm (1996)

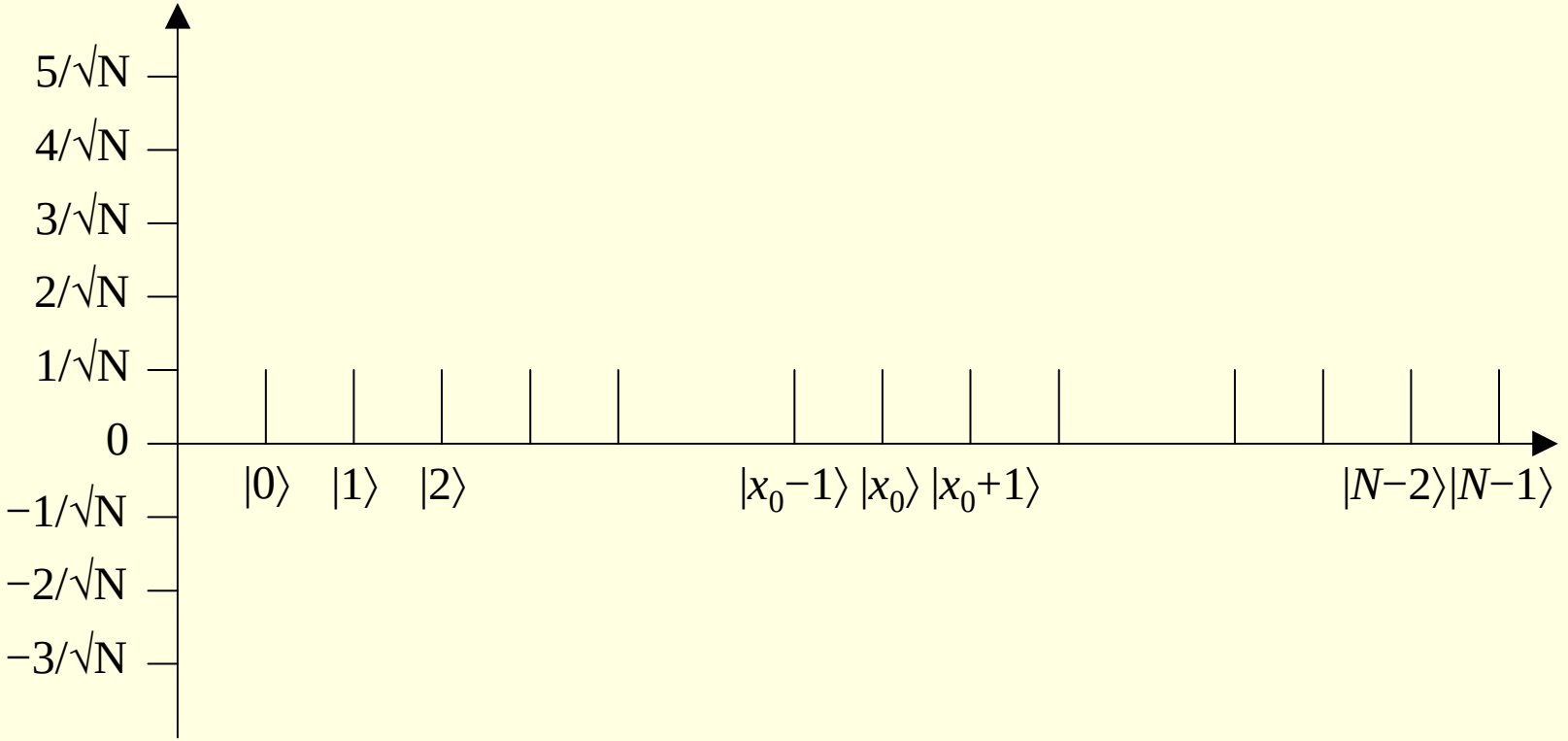


$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle = \left(\frac{1}{\sqrt{N}} \quad \frac{1}{\sqrt{N}} \quad \cdots \quad \frac{1}{\sqrt{N}}\right)^{T}$$

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Efficient quantum algorithm

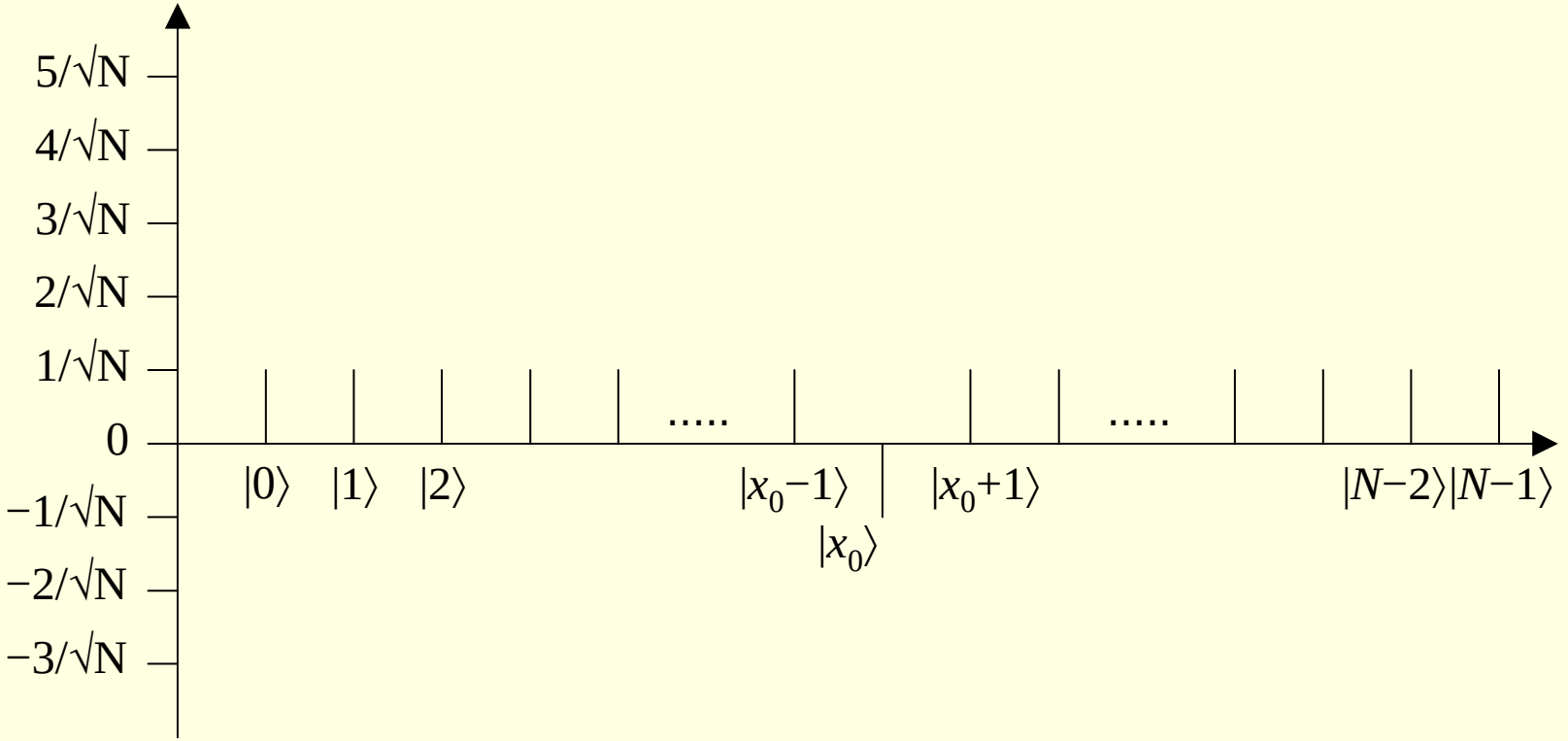
- The values of the components of the state vector



Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Efficient quantum algorithm

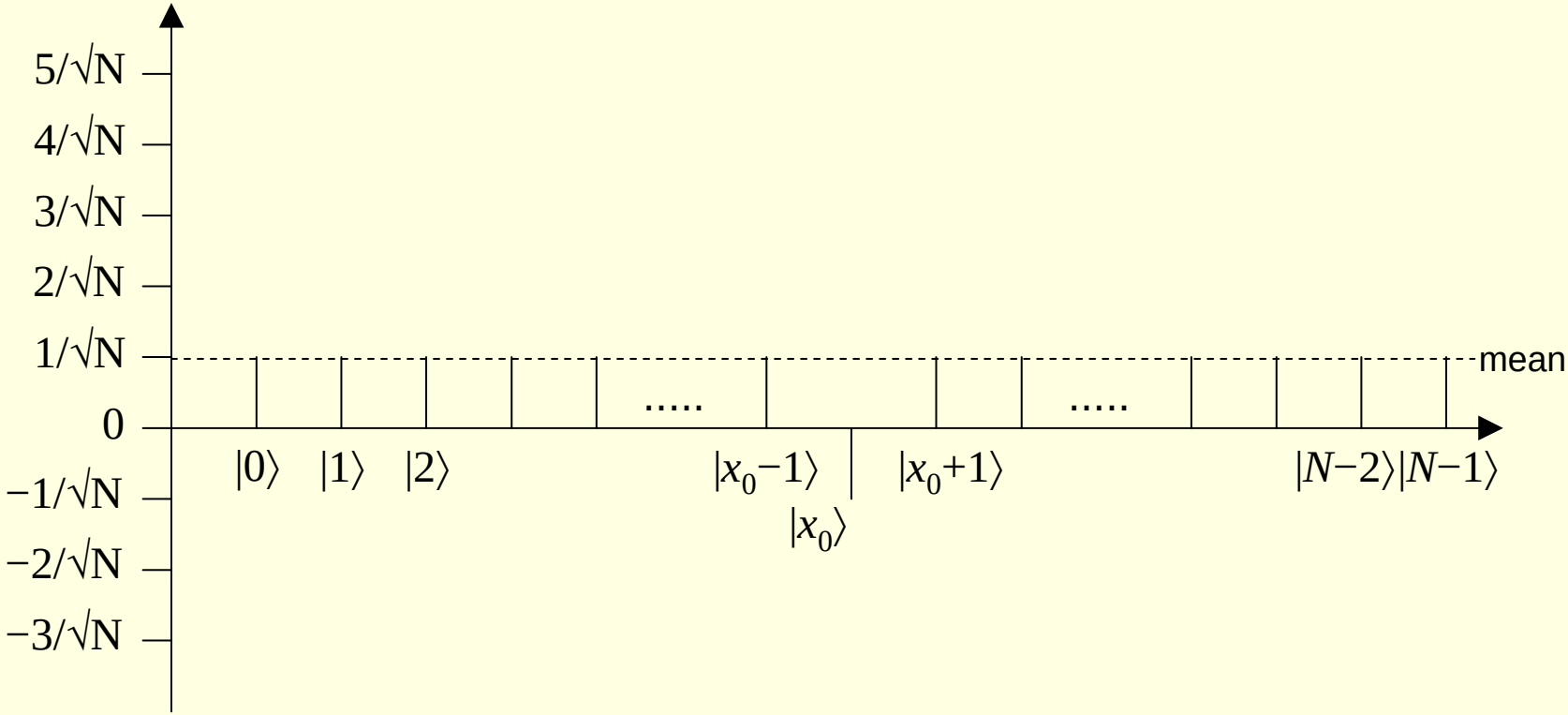
- After the f-query



Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Efficient quantum algorithm

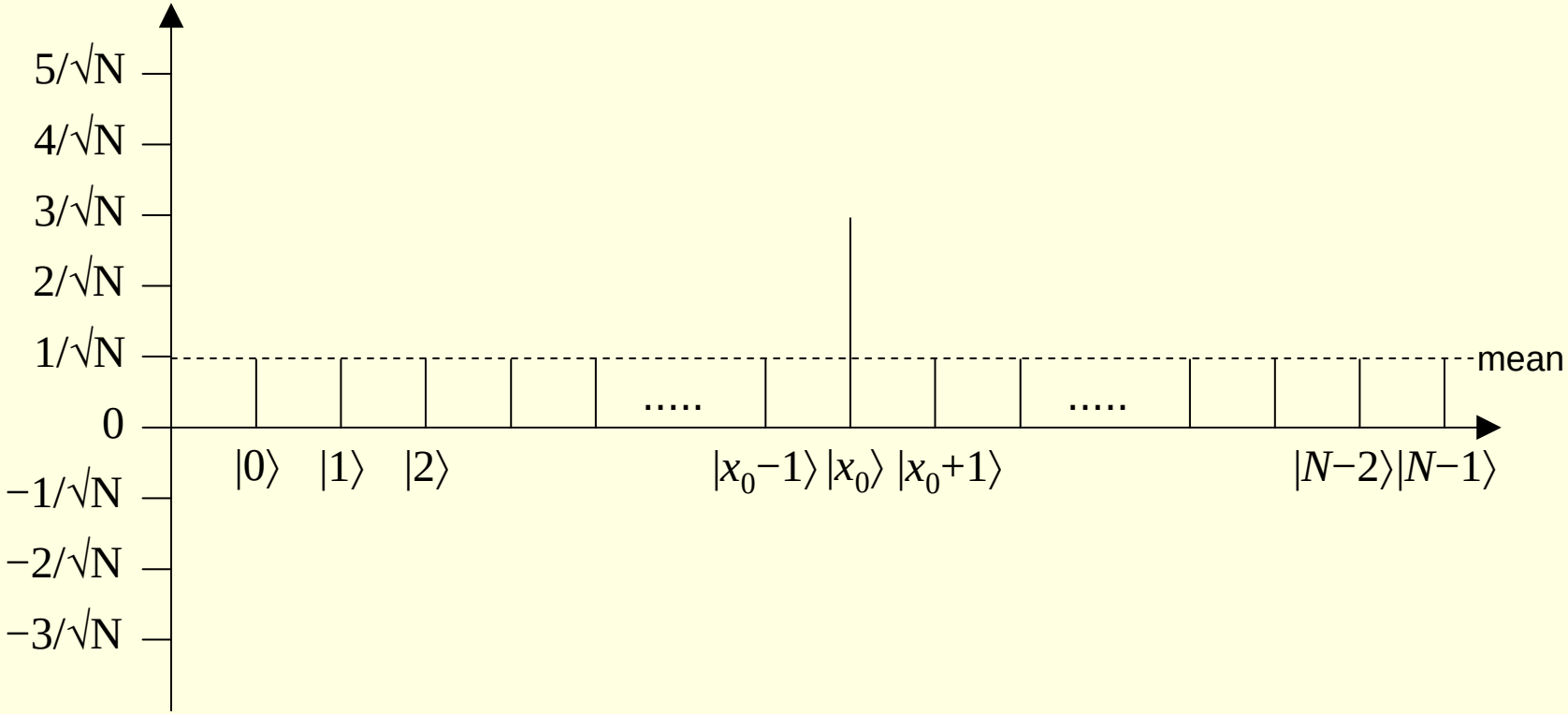
- After the f-query



Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Efficient quantum algorithm

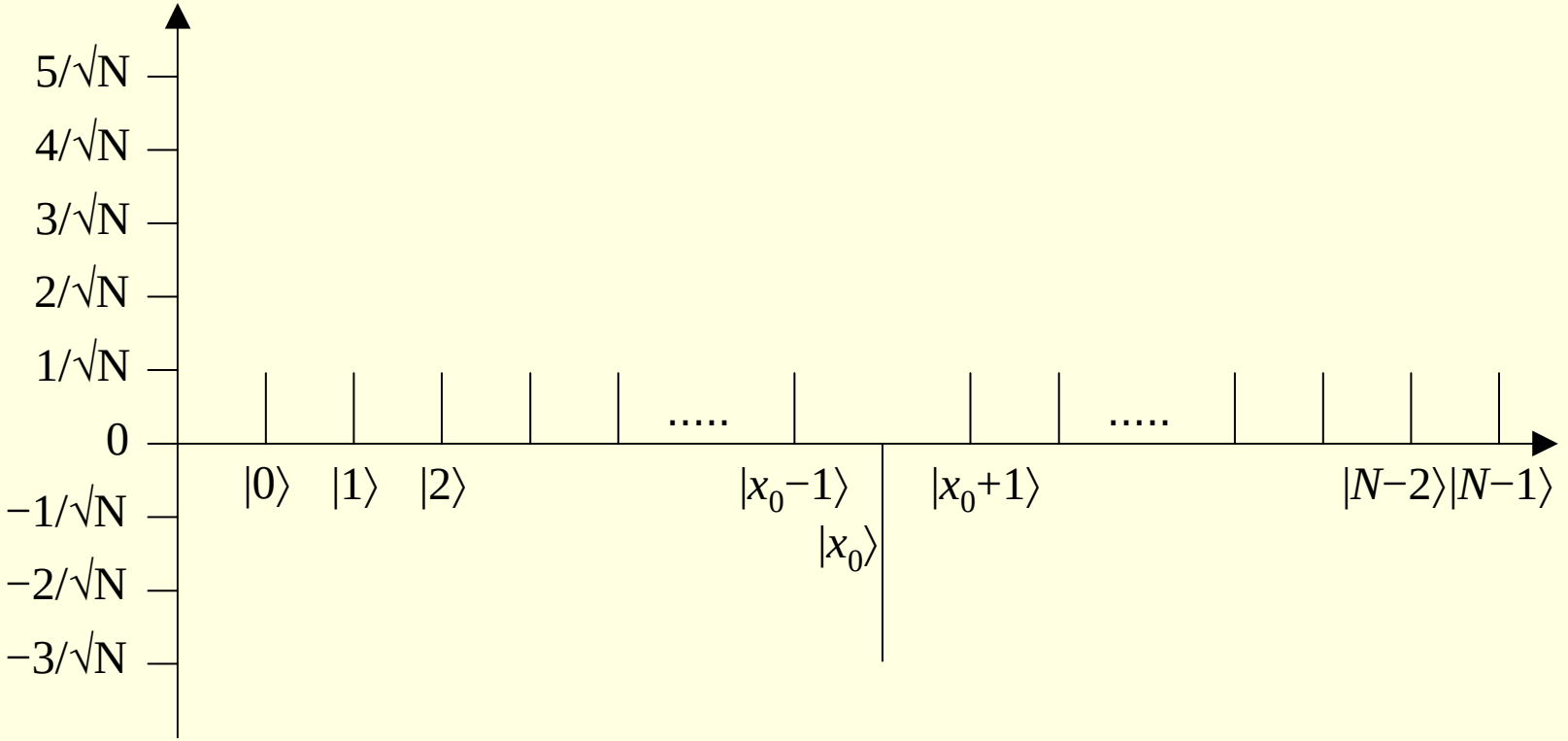
- After the diffusion



Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Efficient quantum algorithm

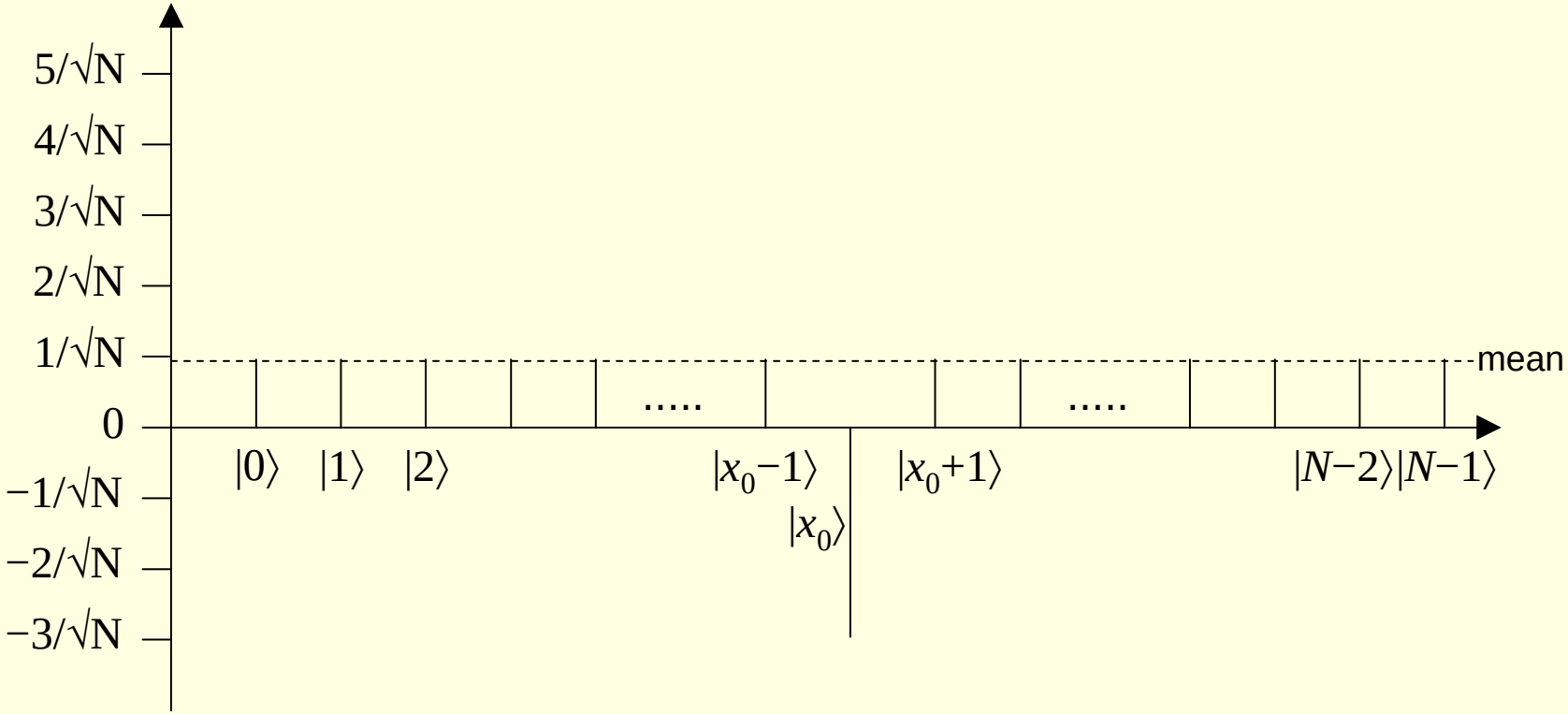
- After the f-query



Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Efficient quantum algorithm

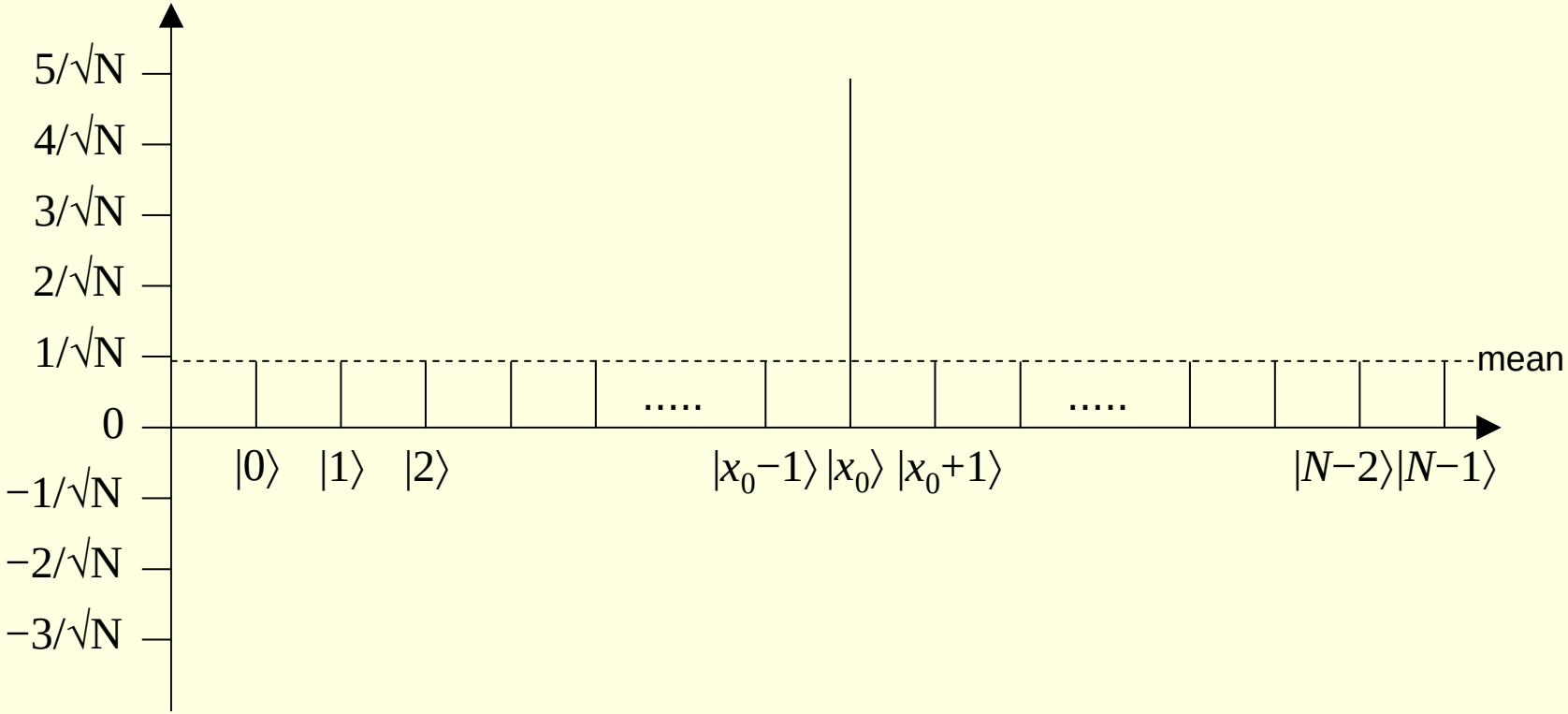
- After the f-query



Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Efficient quantum algorithm

- After the diffusion



Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Efficient quantum algorithm

- After $O(\sqrt{N})$ iterations the amplitude at $|x_0\rangle$ practically reaches 1
- So the measurement at that moment gives $|x_0\rangle$ with probability (almost) 1
- Classically at least $O(N)$ queries are required

ESF EIROPAS SOCIĀLAIS FONDS

Eiropas Sociālā fonda projekts
"Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku"
Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Thank you for your attention!

Questions?

- Eiropas Sociālā fonda projekts
- “Datorzinātnes pielietojumi un tās saiknes ar kvantu fiziku”
- Nr.2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044