Repetition or where are we?

POSTULATES OF QUANTUM MECHANICS FROM ENGINEERING POINT OF VIEW

1th postulate: quantum bit

- Vector in Hilbert space

$$|\varphi\rangle = \sum_{i=0}^{2^n-1} \varphi_i |i\rangle$$

2th postulate : logic gates

- Unitary transform
- Elementary logic gates

$$U^\dagger \equiv U^{-1}$$

3rd postulate : Q/C conversion

- Measurement statistics
- Post measurement state

$$P(m \mid |\varphi\rangle) = \langle\varphi|M_m^\dagger M_m|\varphi\rangle$$

$$|\varphi'\rangle = \frac{M_m|\varphi\rangle}{\sqrt{\langle\varphi|M_m^\dagger M_m|\varphi\rangle}}$$

4th postulate : registers

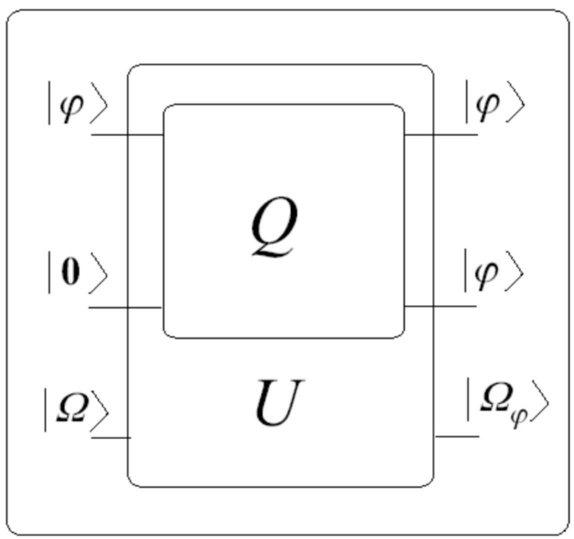
- Tensor product

$$|\varphi\rangle = |0\rangle \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

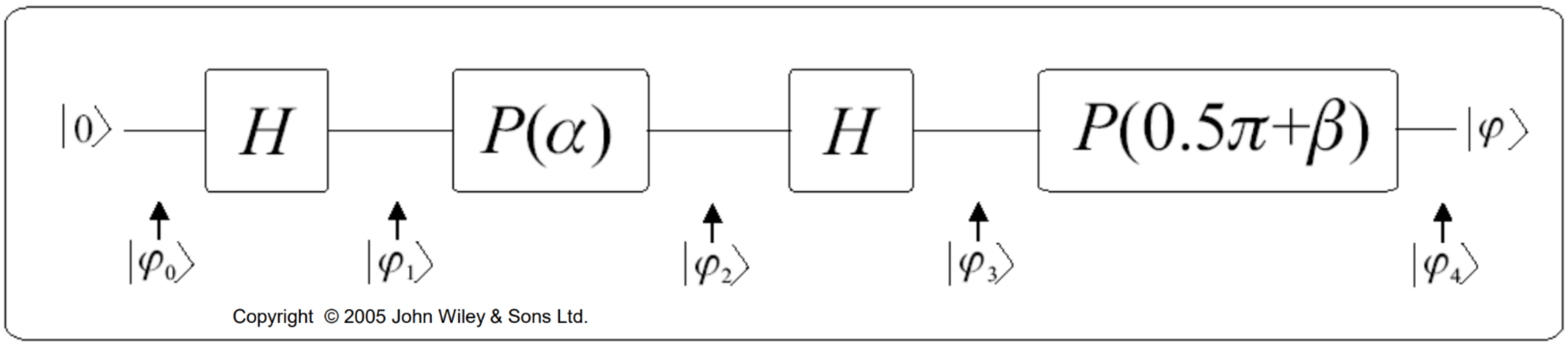
CONSEQUENCES

- Entanglement $|\beta_{00}\rangle = \dfrac{|00\rangle + |11\rangle}{\sqrt{2}}$
  - Einstein: “spooky action at a distance“
  - Einstein: “God does not play dice with the universe.”

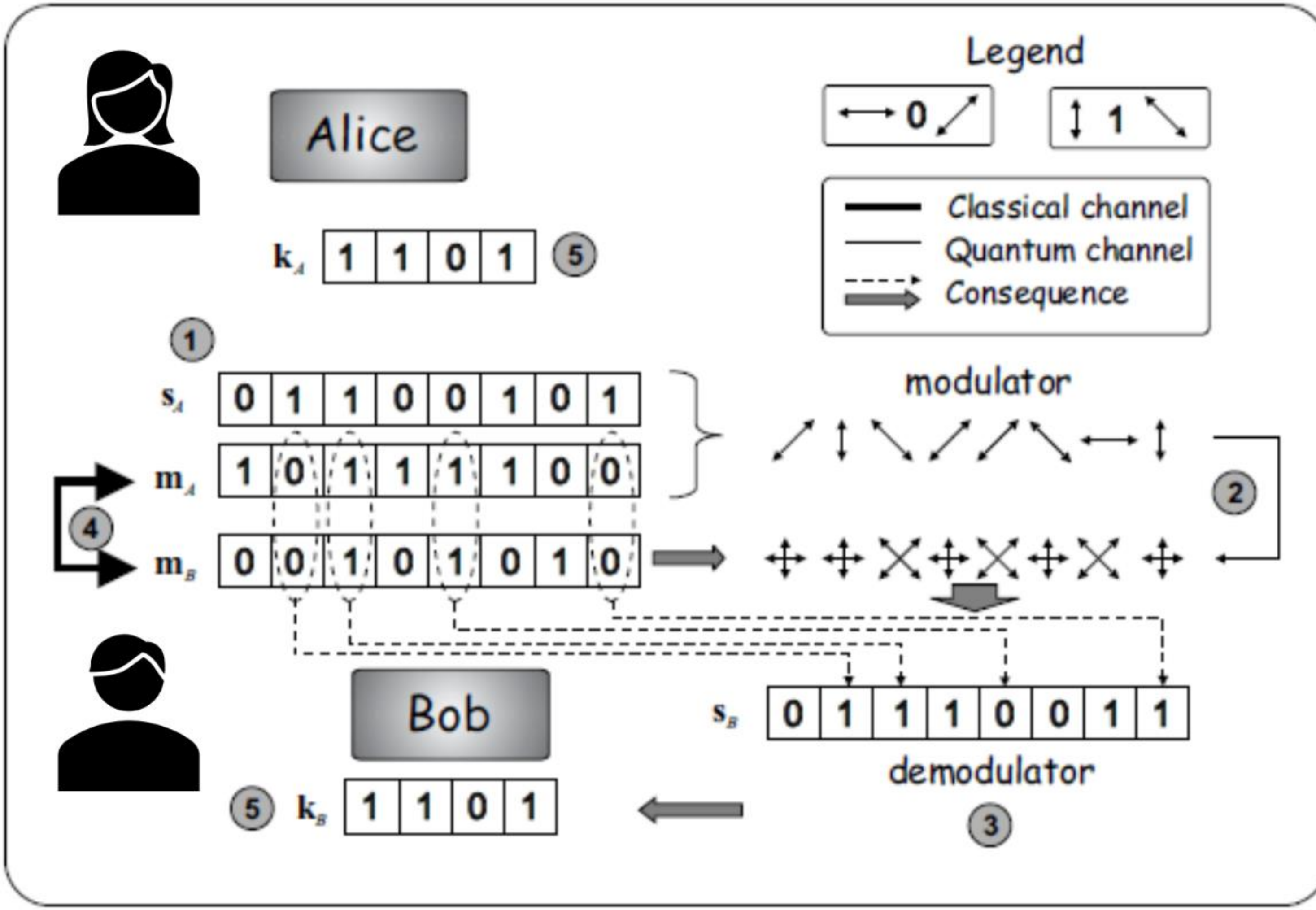
- No cloning theorem



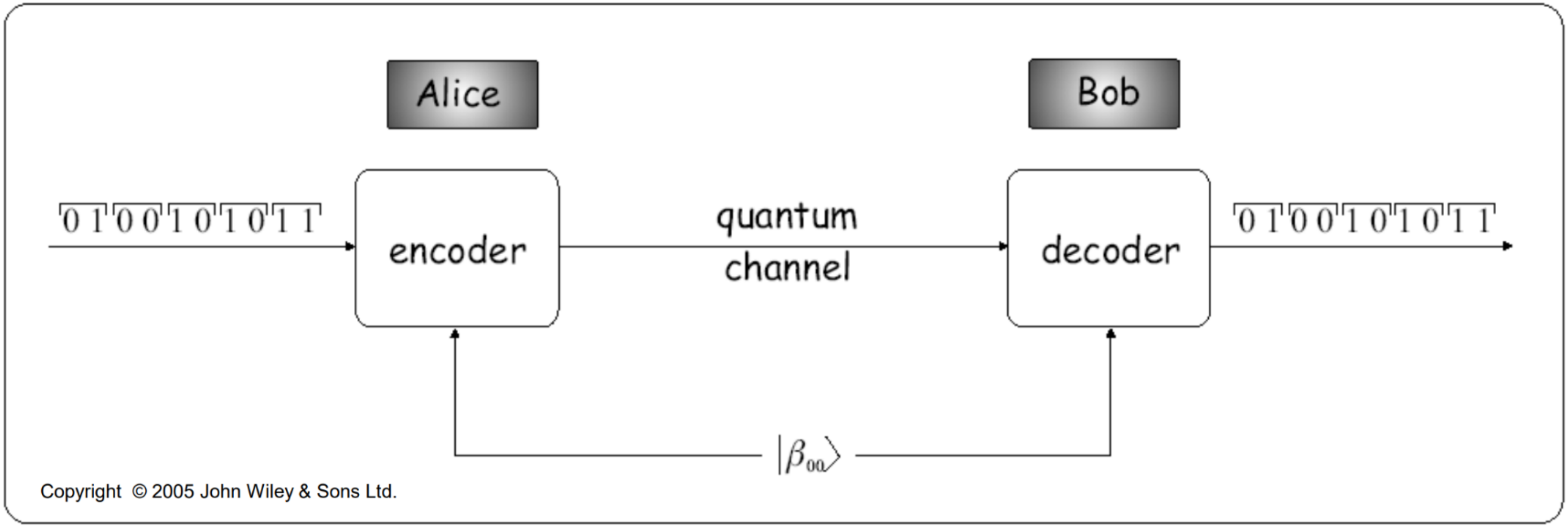
PREPARATION OF ARBITRARY 1-QUBIT STATE



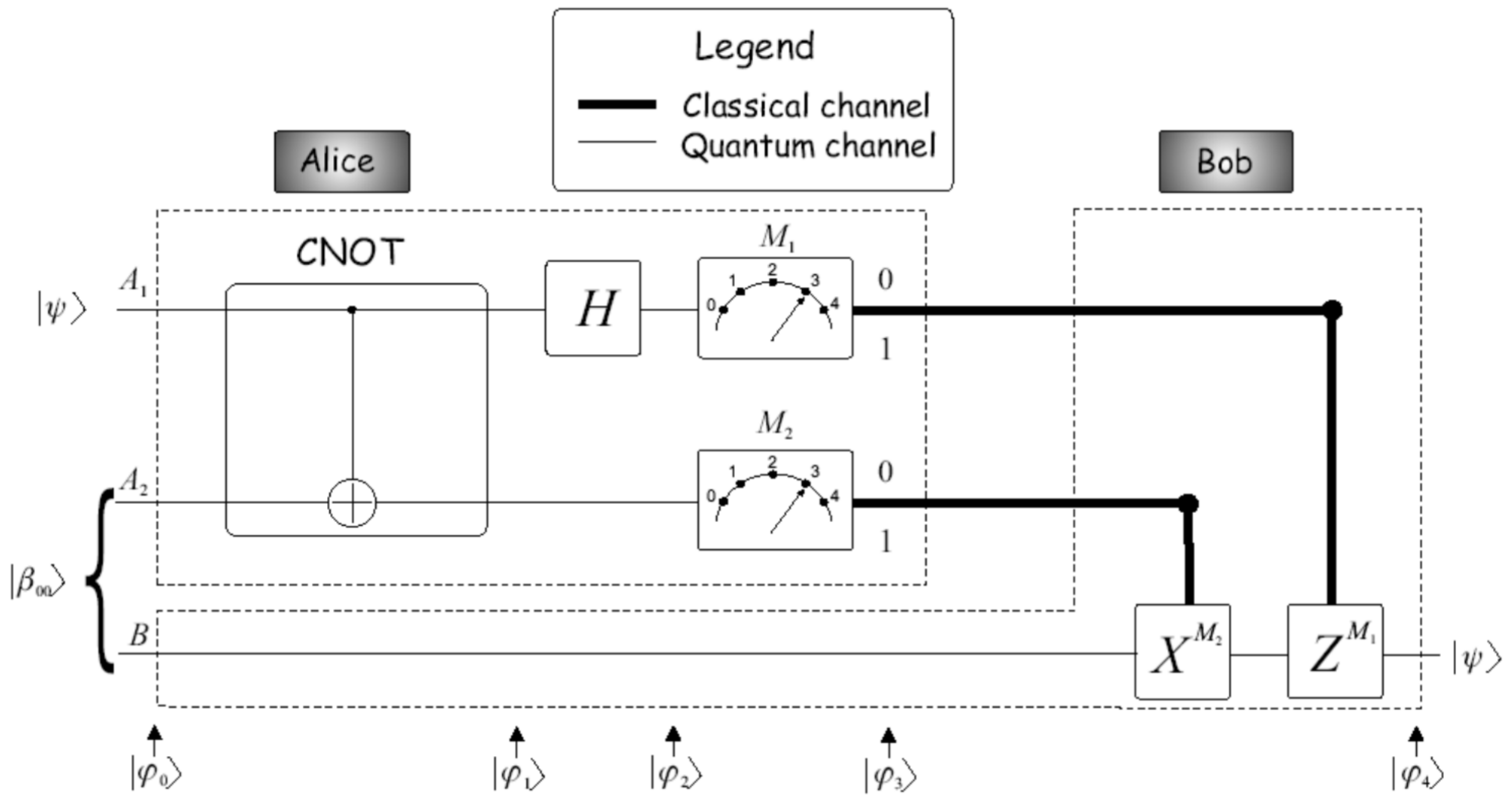
QKD


Legend
0
1
Classical channel
Quantum channel
Consequence
Alice
k_A 1 1 0 1
5
1
s_A 0 1 1 0 0 1 0 1
m_A 1 0 1 1 1 1 0 0
4
m_B 0 0 1 0 1 0 1 0
modulator
2
Bob
s_B 0 1 1 1 0 0 1 1
demodulator
3
5
k_B 1 1 0 1

SUPERDENSE CODING



TELEPORTATION



DEPARTMENT OF
NETWORKED SYSTEMS
AND SERVICES

Quantum parallelism, Deutsch-Jozsa algorithm and QFT

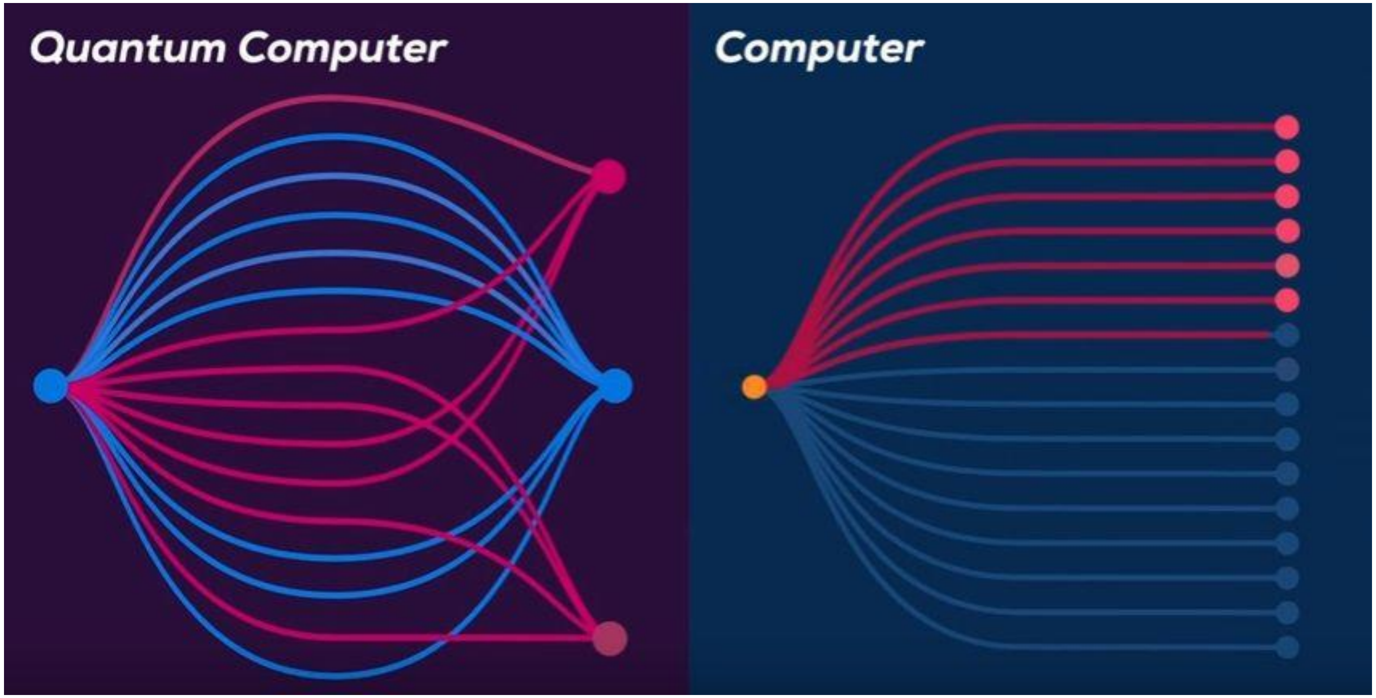
Quantum Computing and its Applications
BMEVIHIAD00, Spring 2025

Dr. László Bacsárdi, Dr. Sándor Imre

Department of Networked Systems and Services
Budapest University of Technology and Economics
bacsardi@hit.bme.hu

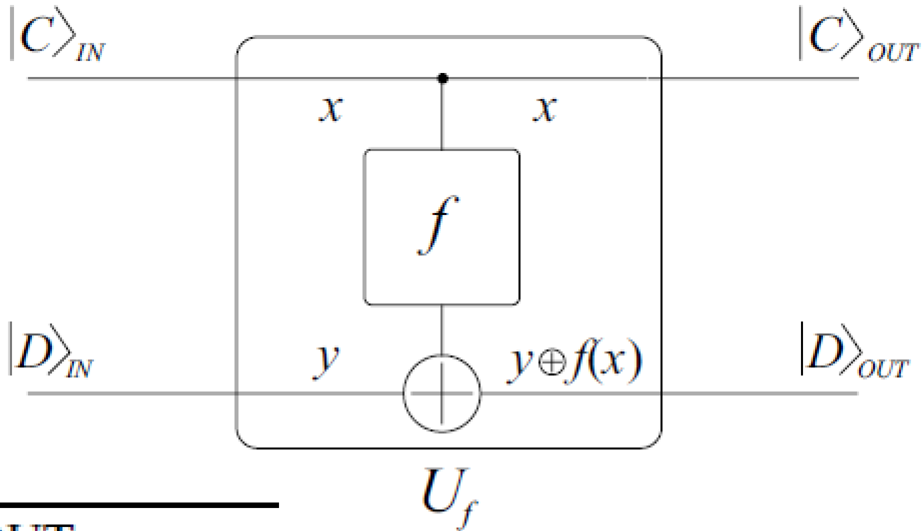
MŰEGYETEM 1782

Quantum parallelism



steemit

$$U_f : |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$$

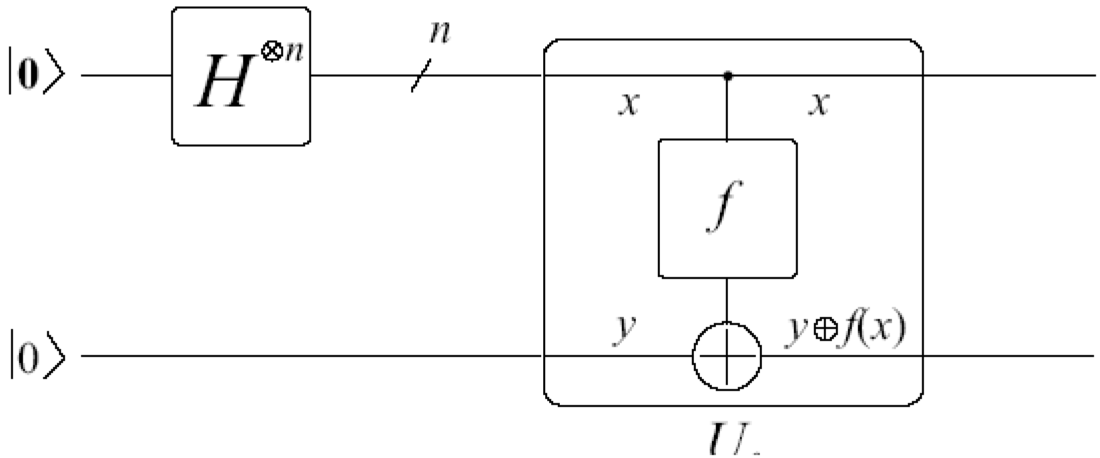


IN		OUT	
x	y	x	$y \oplus f(x)$
0	0	0	$0 \oplus f(0) = f(0)$
0	1	0	$1 \oplus f(0)$
1	0	1	$0 \oplus f(1) = f(1)$
1	1	1	$1 \oplus f(1)$

$$U_f \frac{|00\rangle + |10\rangle}{\sqrt{2}} = \frac{|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle}{\sqrt{2}}$$

KVANTUM PÁRHUZAMOSSÁG

Egy lépesben kis $U_f : |x\rangle_N |y\rangle \rightarrow |x\rangle_N |y \oplus f(x)\rangle$

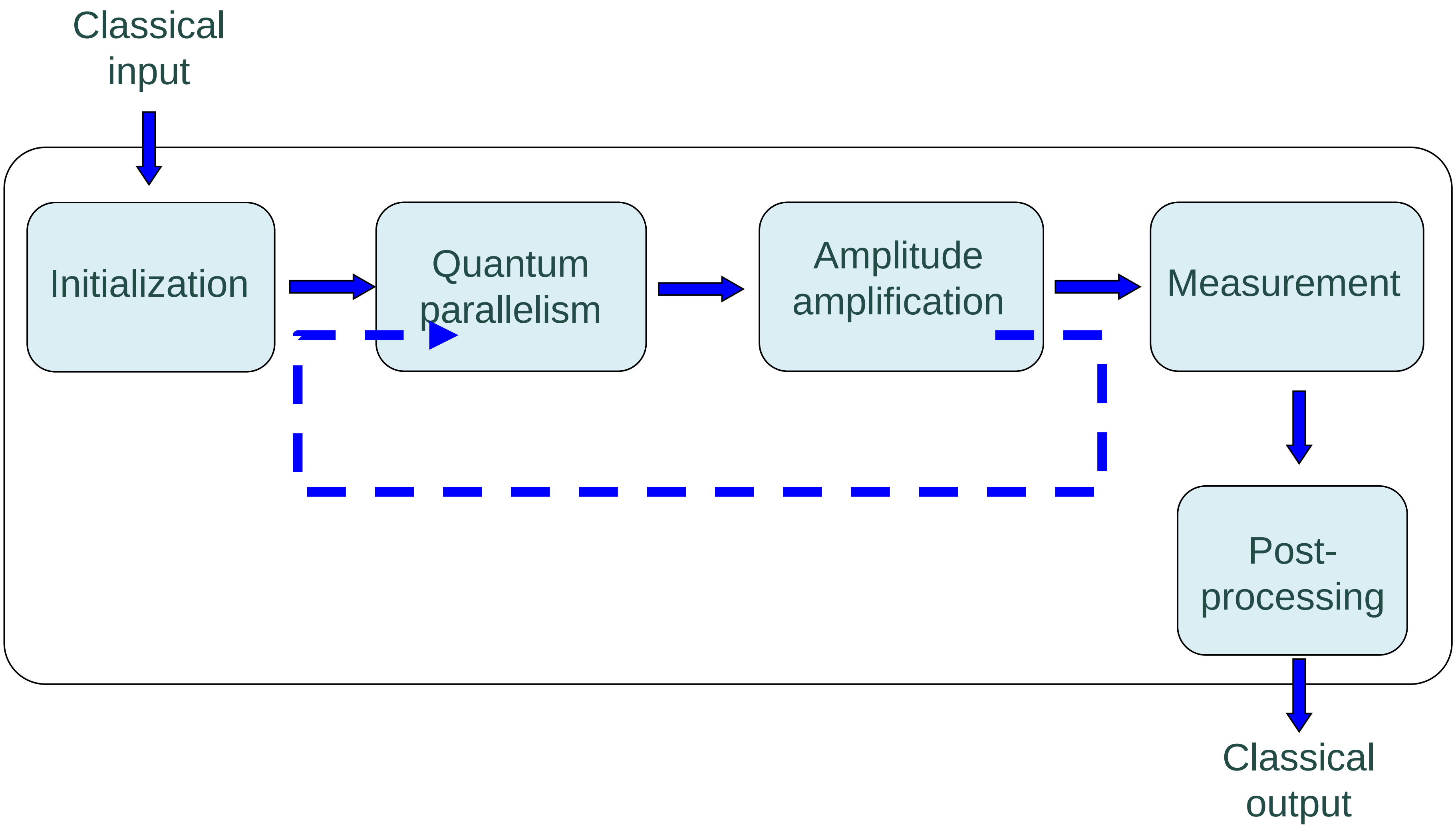


In 1 step for every *x*!

$$U_f \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |0 \oplus f(x)\rangle$$

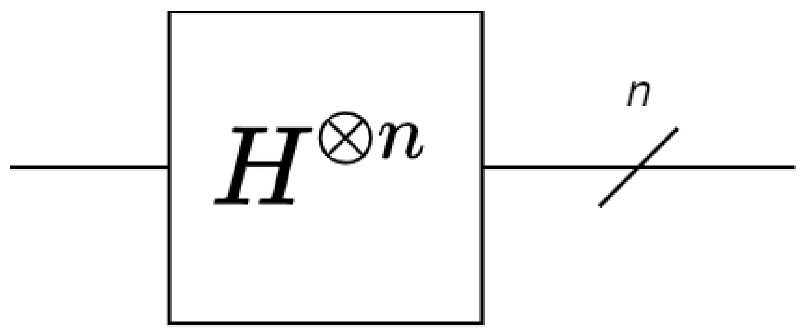
$$= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n - 1} |x\rangle |f(x)\rangle$$

GENERAL RECIPE FOR QUANTUM ALGORITHM DESIGN



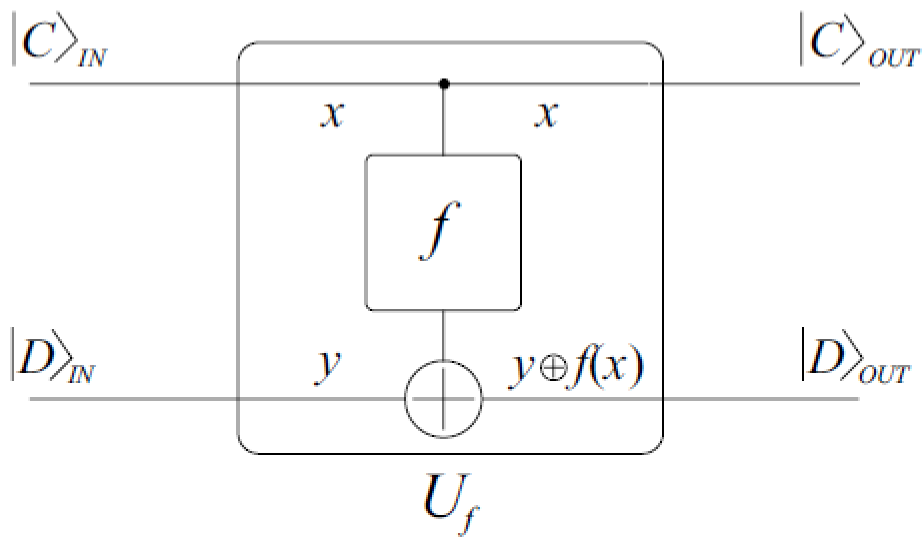
INITIALIZATION

- The initialization of the circuit in a quantum manner:
  - Generating a superposition state having uniform probability distribution. All the integer numbers (basis vectors) in the superposition have the same amplitude, i.e., we give the same chance to each of them to be selected.



QUANTUM PARALLELIZM

- We evaluate a function/operation for each input integer number contained by the superposition in one single step.
- Or sometimes in several steps ☺.



AMPLITUDE AMPLIFICATION

- It modifies the superposition in such a way that the marked/requested integer number/basis vector gets a probability amplitude 1 or close to 1.
- This guarantees that the measurement will give back the requested integer with high probability. This guarantees that the measurement will most likely return the desired value.
- Amplitude amplification can be achieved in most cases in a single step, using the Hadamard transform or Quantum Fourier Transform. But it can also be iterative (i.e. requiring multiple steps).
- There is no clear recipe for amplitude amplification. We can only show examples. This step requires the greatest creativity and intuition.

MEASUREMENT

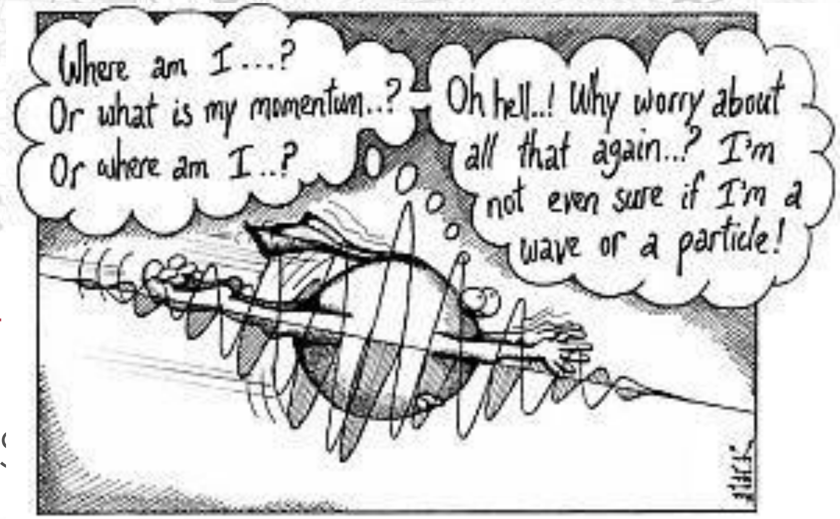
- Already discussed within the postulates of quantum mechanics.
- Carefully set measurement operators guaranties the proper measurement result.

$$P(m \mid |\varphi\rangle) = \langle\varphi|M_m^\dagger M_m|\varphi\rangle$$

$$|\varphi'\rangle = \frac{M_m|\varphi\rangle}{\sqrt{\langle\varphi|M_m^\dagger M_m|\varphi\rangle}}$$

CLASSICAL POSTPROCESSING

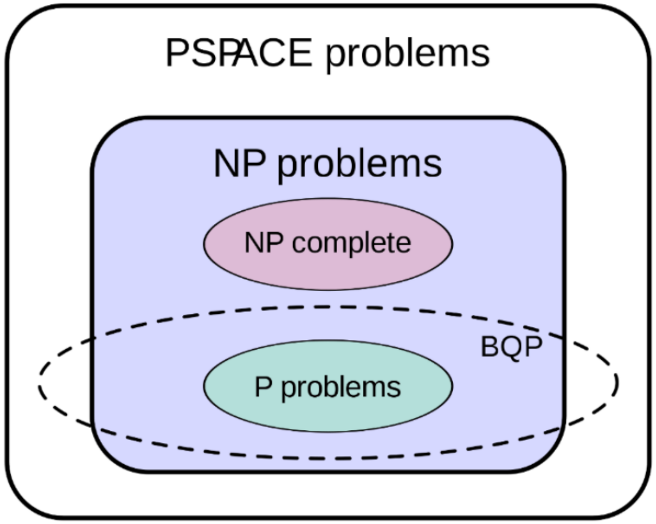
- During post-processing, the measurement result is transformed into a solution to the initial problem
- In most cases, post-processing involves simply reporting the measured value.
- However, sometimes complex mathematical derivations are required.



Photon self-identity problems.

The Deutsch-Józsa algorithm

- P: polynomial time
- NP: nondeterministic, polynomial time
- BQP: bounded error, quantum, polynomial time
- PSACE: polynomial amount of space

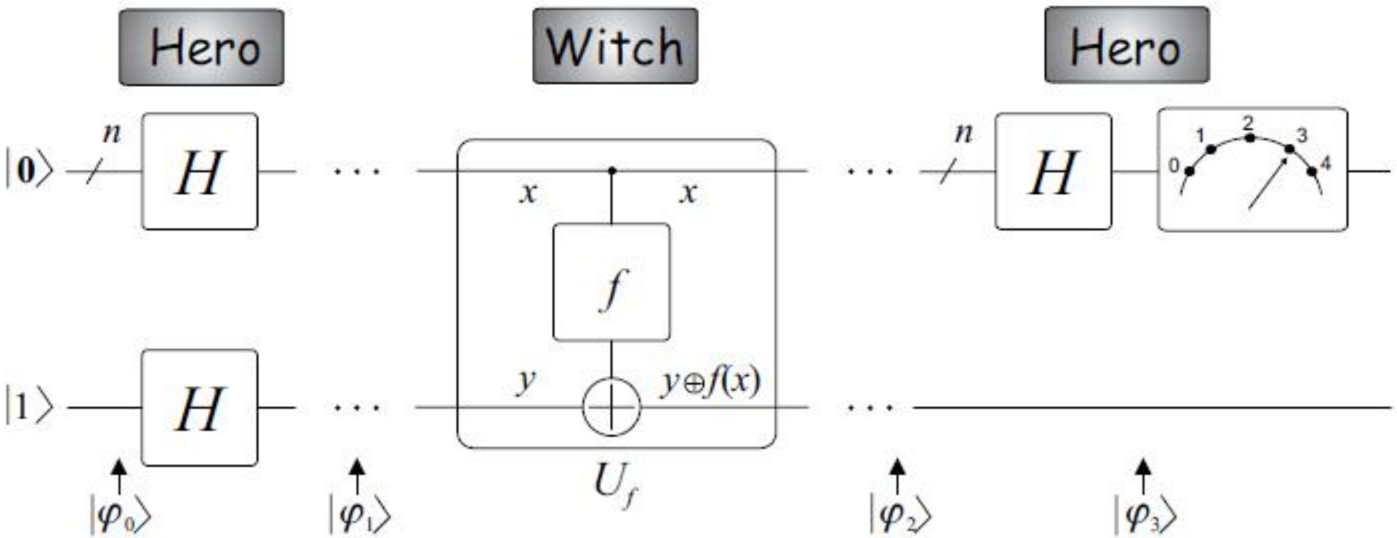


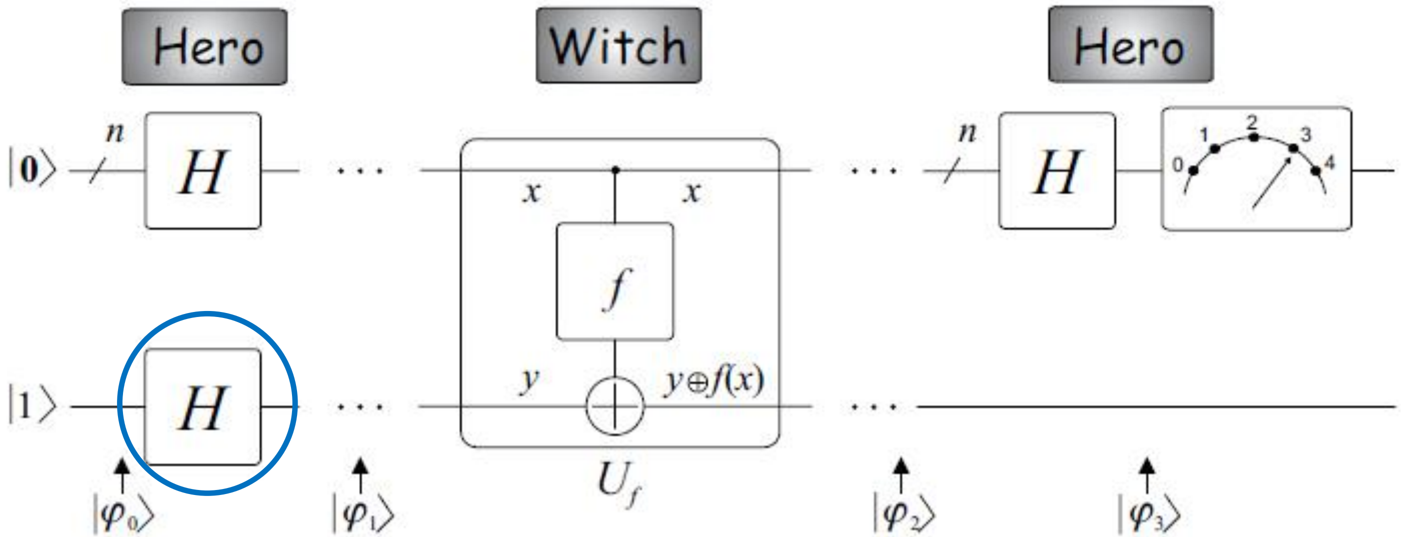
THE DEUTSCH-JÓZSA ALGORITHM

- Constant or balanced?
- Best classical solution?

$$x \in \{0,1\}^n$$

$$f(x) : \{0,1\}^n \to \{0,1\}^1$$

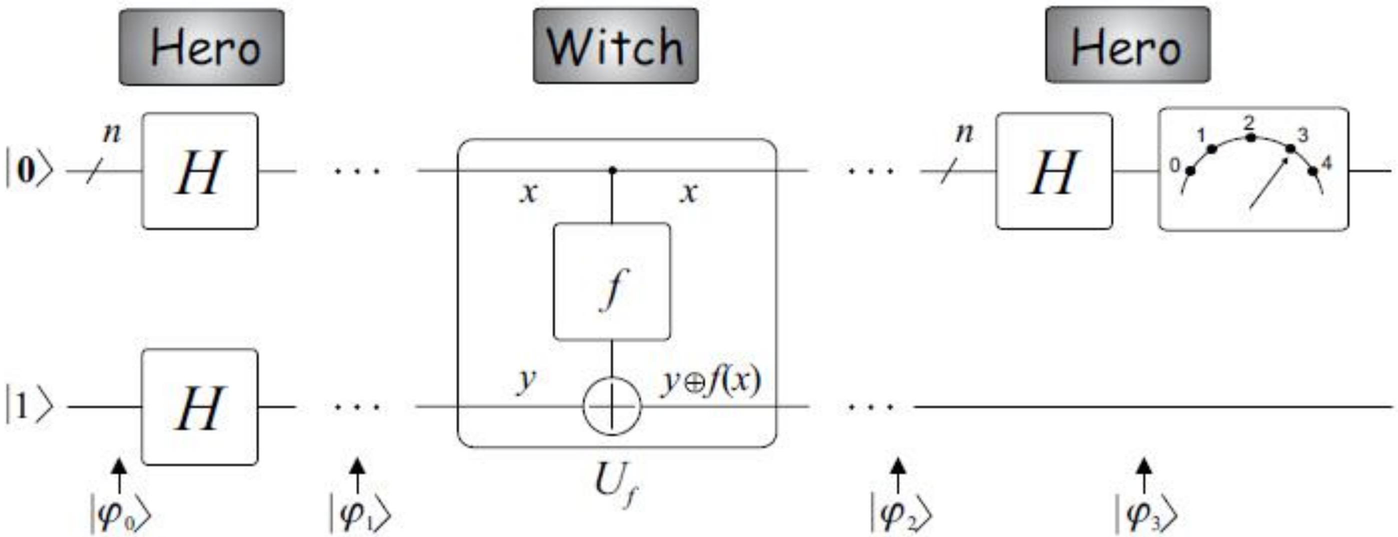




$$|\varphi_0\rangle = |0\rangle_N |1\rangle$$

$$|\varphi_1\rangle = H^{\otimes(n+1)}|\varphi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$= \frac{1}{\sqrt{2^{(n+1)}}} \sum_{x\in\{0,1\}^n} |x\rangle|0\rangle - \frac{1}{\sqrt{2^{(n+1)}}} \sum_{x\in\{0,1\}^n} |x\rangle|1\rangle$$

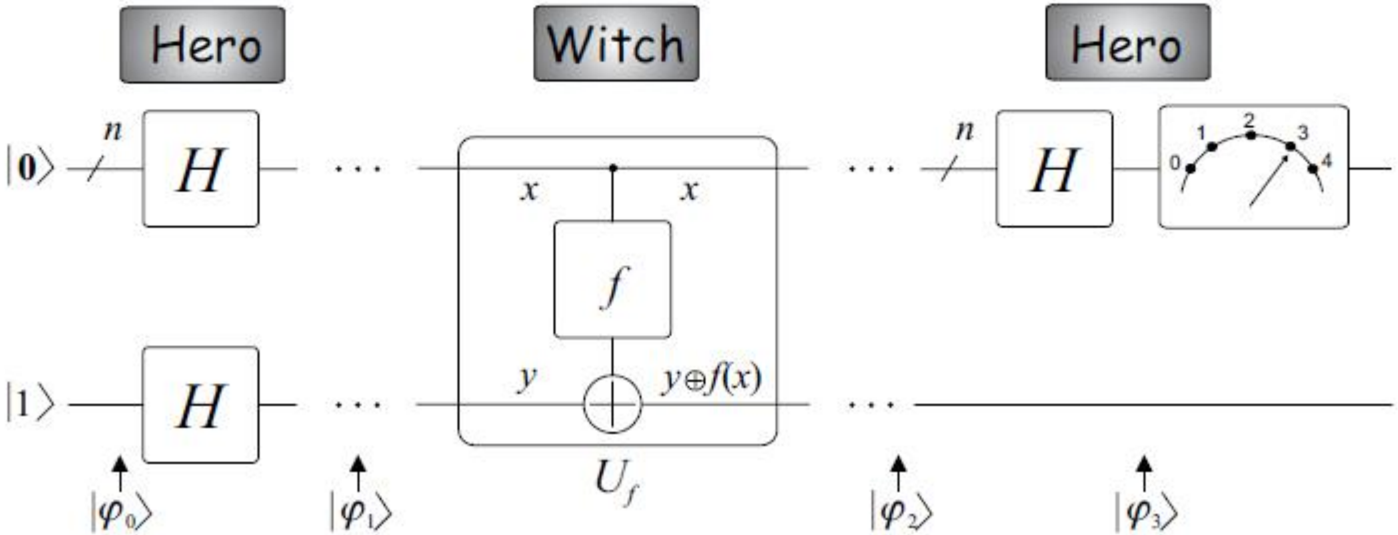


- First term (already known):

$$U_f \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|0 \oplus f(x)\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|f(x)\rangle$$

www.hit.bme.hu



- Second term:

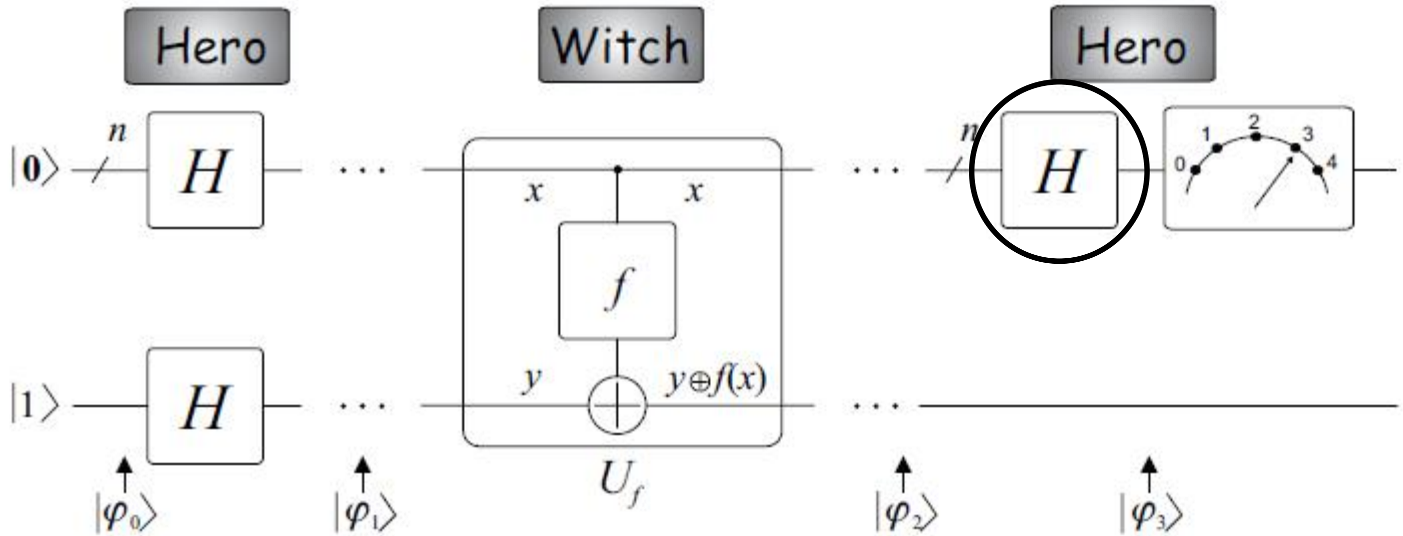
$$U_f \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|1\oplus f(x)\rangle$$

$$|\varphi_2\rangle = U_f|\varphi_1\rangle = \frac{1}{\sqrt{2^{(n+1)}}} \sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle - \frac{1}{\sqrt{2^{(n+1)}}} \sum_{x\in\{0,1\}^n} |x\rangle|1\oplus f(x)\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \frac{|f(x)\rangle - |1\oplus f(x)\rangle}{\sqrt{2}}$$

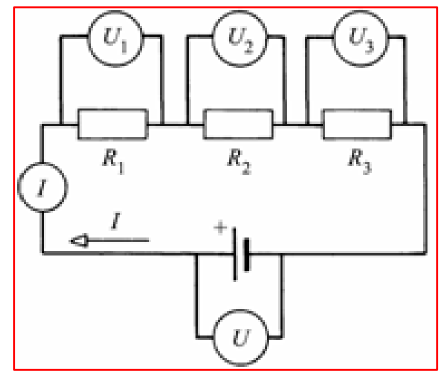
$$= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

HF



$$\boxed{H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} (-1)^{xz}|z\rangle}$$

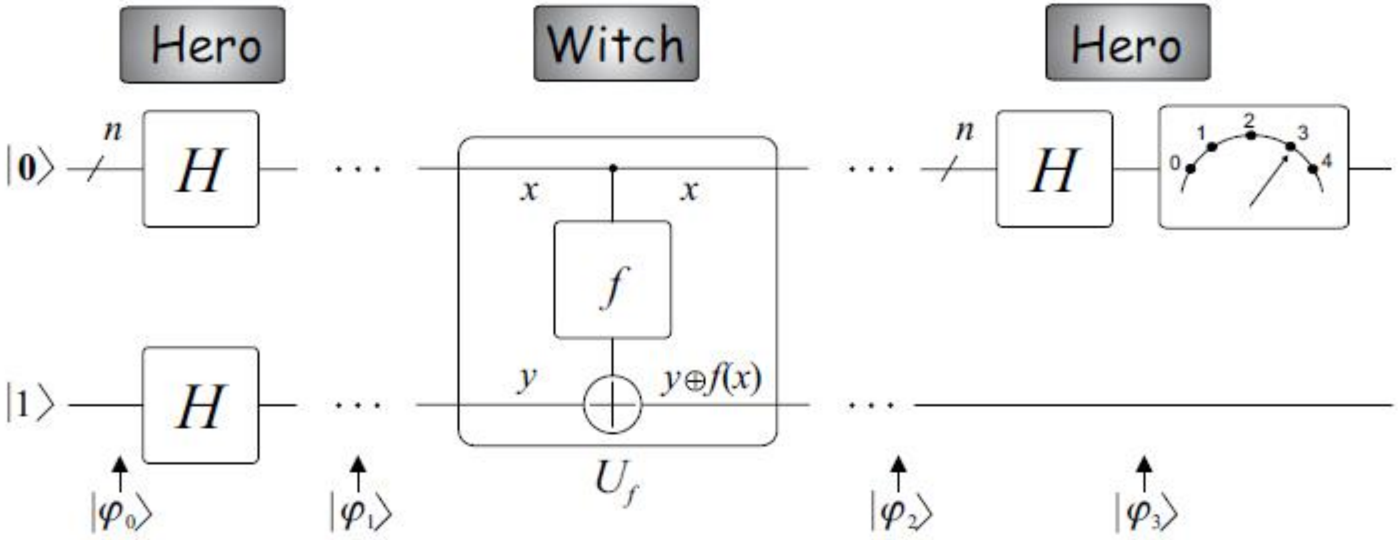
Application of superposition principle



$$|\varphi_3\rangle = (H^{\otimes n}\otimes I)|\varphi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} H^{\otimes n}|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \frac{1}{\sqrt{2^n}} \sum_{x'\in\{0,1\}^n} (-1)^{xx'}|x'\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$= \sum_{x'\in\{0,1\}^n} \underbrace{\left(\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{xx'+f(x)} \right)}_{c_{x'}} |x'\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$



$$c_0 = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{xx' + f(x)} = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)}$$

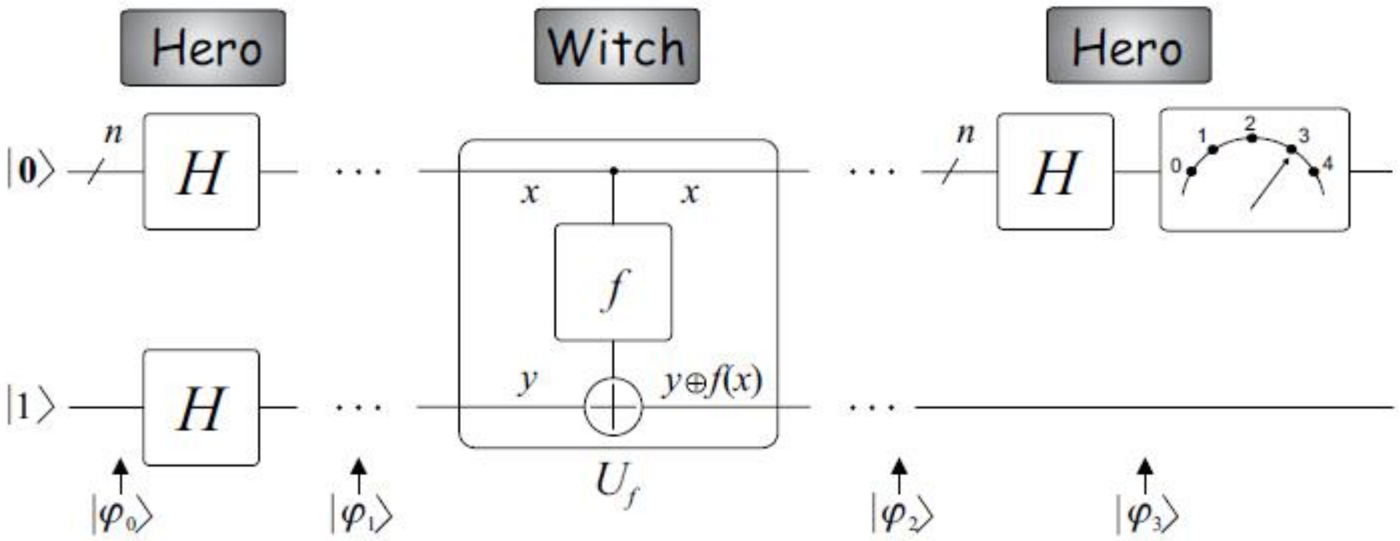
since $xx' = x\mathbf{0} \equiv 0$. Now let us investigate (5.10) when $f(x)$ is *constant*, then

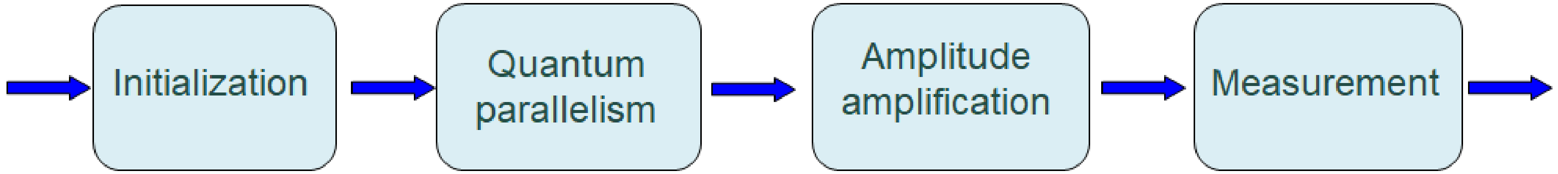
$$c_0 = \begin{cases} -1 & \text{if } f(x) \equiv 1 \\ 1 & \text{if } f(x) \equiv 0. \end{cases}$$

(

Concerning the *balanced* scenario $c_0 = 0$ since we have the same number of positive (+1) and negative (-1) terms in the sum.

DESIGN MODEL FOR QUANTUM ALGORITHMS

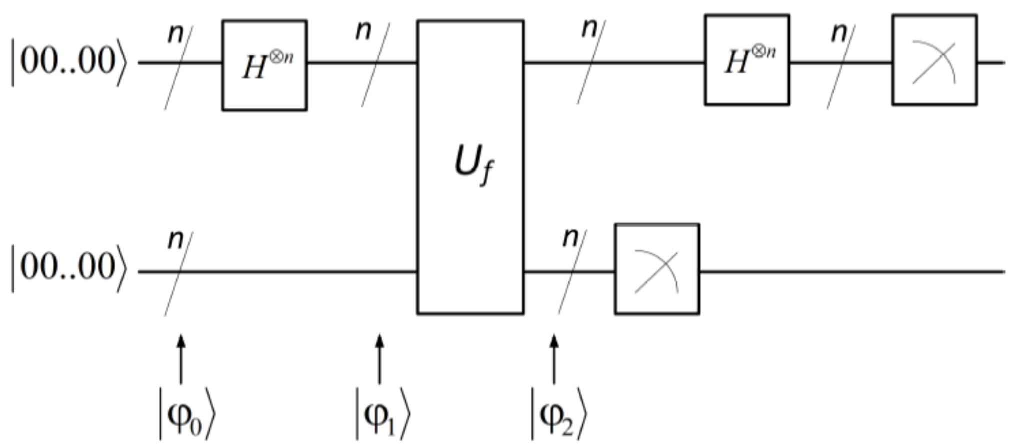




SIMON-ALGORITMUS

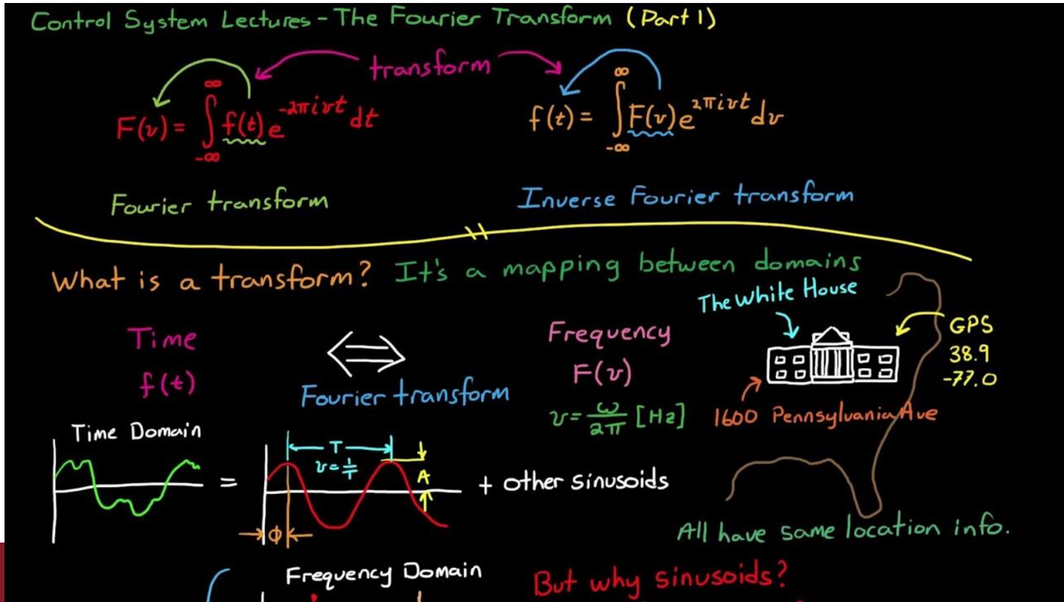
Let us modify the function f and the related question under discussion in the Deutsch–Jozsa problem in the following way: $f : \{0,1\}^n \rightarrow \{0,1\}^n$, i.e. Simon's algorithm deals with a binary vector valued function which is constrained by a special condition. f is periodical in terms of $f(x) = f(y)$ if and only if $x = y$ or $x = y \oplus r$, where $r \neq 0$ stands for the binary period of f. There are two obvious questions, namely how and in how many steps (evaluation of f) can r be computed. These questions can answered both classically and quantum computationally but with a major difference. A traditional computer requires an exponential number of queries while Simon's solution is able to find r after $O(n)$ iterations with high probability.

$$x \in \{0,1\}^n$$
$$f(x) : \{0,1\}^n \rightarrow \{0,1\}^n$$
$$f(x) = x \oplus s$$

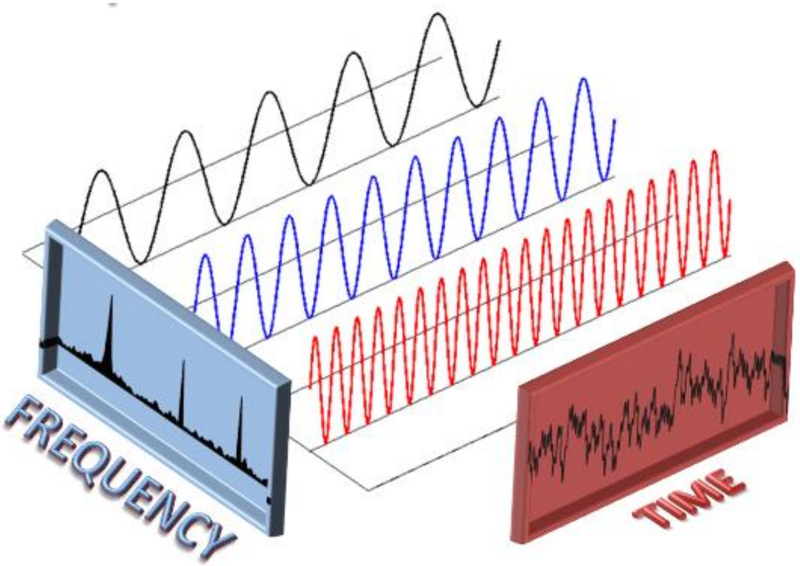


DEPARTMENT OF NETWORKED SYSTEMS AND SERVICES

Quantum Fourier Transform



FOURIER Jean Baptiste Joseph (1768-1830)



- Classical Discrete Fourier Transform (DFT)

$$\mathbf{x} = [x_0, x_1, ..., x_{N-1}]^T \quad x_i \in \mathbb{C}$$

$$\mathbf{y} = \mathrm{DFT}\{\mathbf{x}\}$$

$$y_k \triangleq \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} x_i e^{j\frac{2\pi}{N}ik}$$

- Quantum Discrete Fourier Transform (QFT)

$$|\varphi\rangle = \sum_{i=0}^{N-1} \varphi_i |i\rangle$$

$$\boxed{\psi_k \triangleq \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} \varphi_i e^{j\frac{2\pi}{N}ik}}$$

$$|\psi\rangle = F|\varphi\rangle$$

Exercise 6.1. Prove that operator F is unitary!

Exercise 6.2. Determine the matrix of QFT!

DEFINITIONS

- For computational basis states

$$F|i\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{j\frac{2\pi}{N}ik} |k\rangle$$

- For arbitrary superposition

$$|\psi\rangle = \sum_{k=0}^{N-1} \psi_k |k\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \sum_{i=0}^{N-1} \varphi_i e^{j\frac{2\pi}{N}ik} |k\rangle$$

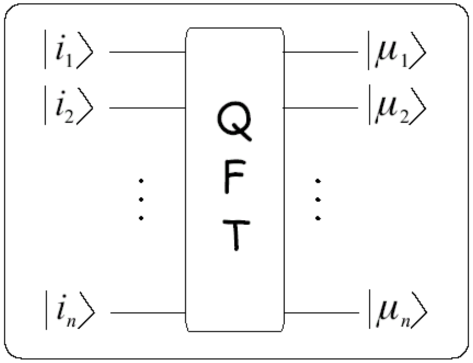
- Inverse Fourier Transform (IQFT)

$$\varphi_i \triangleq \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \psi_k e^{-j\frac{2\pi}{N}ik}$$

$$\boxed{F^\dagger|k\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} e^{-j\frac{2\pi}{N}ik} |i\rangle}$$

HOW TO IMPLEMENT QFT 1

- The goal: to find an efficient circuit implementing QFT built from elementary quantum gates.
- The way: we prepare an equivalent tensor product representation of QFT which advises us what shall we do on each quantum wire separately.



- Binary representation of integer and real numbers:

An integer number $k \in \{0, 1, ..., 2^n - 1\}$ can be represented in the binary form of $(k_1, k_2, .., k_n) = k_1 2^{n-1} + k_2 2^{n-2} + ... + k_n 2^0$, where $k_l \in \{0, 1\}$. Let us introduce moreover for $h \geq 0$ the binary notation of

$$0.k_l k_{l+1} ... k_{l+h} \triangleq \frac{k_l}{2^1} + \frac{k_{l+1}}{2^2} + ... + \frac{k_{l+h}}{2^{h+1}}; k_m \in \{0, 1\}.$$

HOW TO IMPLEMENT QFT 2

- Now, we start the reformulation from the original definition

$$F|i\rangle = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{j\frac{2\pi}{N}ik}|k\rangle = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1} e^{j2\pi i\sum_{l=1}^{n} k_l \frac{2^{n-l}}{2^n}}|k\rangle$$

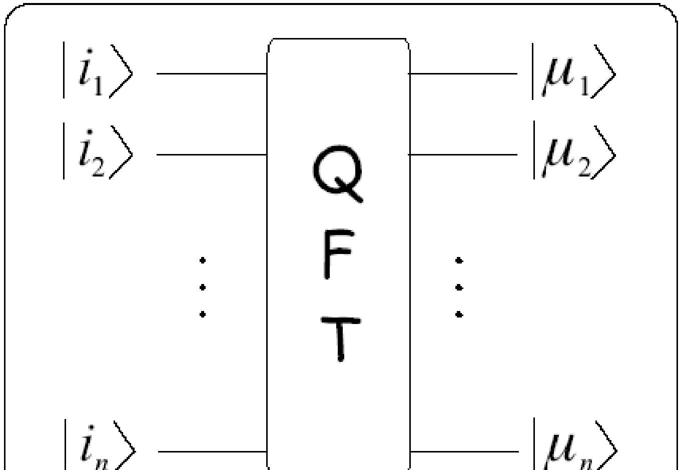
Recognizing that $\frac{2^{n-l}}{2^n} = 2^{-l}$ furthermore exploiting that $|k\rangle = |k_1, k_2, .., k_n\rangle = |k_1\rangle \otimes |k_2\rangle \otimes ... \otimes |k_n\rangle$ and $e^{\alpha+\beta} \equiv e^{\alpha}e^{\beta}$

$$F|i\rangle = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}\prod_{l=1}^{n} e^{j2\pi i k_l 2^{-l}} \bigotimes_{l=1}^{n}|k_l\rangle = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}\bigotimes_{l=1}^{n} e^{j2\pi i k_l 2^{-l}}|k_l\rangle$$

HOW TO IMPLEMENT QFT 3

Considering that $k_l \in \{0,1\}$ we collect the factors of the tensor product into two groups whit respect to $|0\rangle$ and $|1\rangle$

$$F|i\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \left(e^{j2\pi i (k_l=0) 2^{-l}} |0\rangle + e^{j2\pi i (k_l=1) 2^{-l}} |1\rangle \right) = \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \left(|0\rangle + e^{j2\pi i 2^{-l}} |1\rangle \right)$$

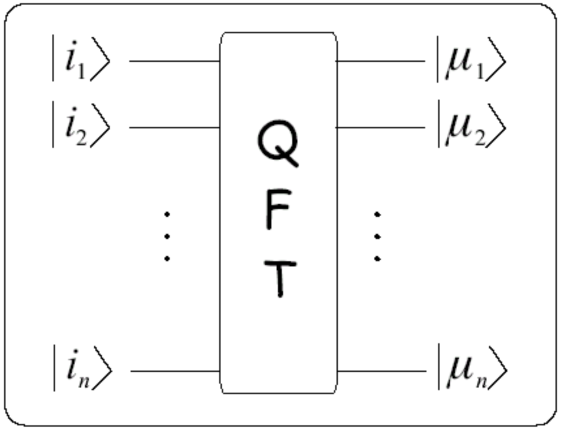


HOW TO IMPLEMENT QFT 4

$$\boxed{|\mu_l\rangle \triangleq \frac{1}{\sqrt{2}}\left(|0\rangle + e^{j2\pi i 2^{-l}}|1\rangle\right)}$$

$$i = \sum_{l=1}^{n} i_l 2^{n-l}$$

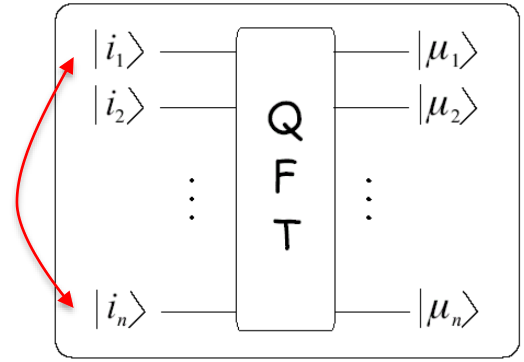
$$\left(2\pi i 2^{-l}\right) \mod 2\pi = 0.i_{l-n} i_{l-n+1} \ldots i_n$$



$$F|i\rangle = \underbrace{\left(\frac{|0\rangle + e^{j2\pi 0.i_n}|1\rangle}{\sqrt{2}}\right)}_{|\mu_1\rangle} \otimes \underbrace{\left(\frac{|0\rangle + e^{j2\pi 0.i_{n-1}i_n}|1\rangle}{\sqrt{2}}\right)}_{|\mu_2\rangle} \otimes \ldots \otimes \underbrace{\left(\frac{|0\rangle + e^{j2\pi 0.i_1 i_2 \ldots i_n}|1\rangle}{\sqrt{2}}\right)}_{|\mu_n\rangle} \tag{6.10}$$

HOW TO IMPLEMENT QFT 4

- Now, we have the tensor product representation in our hand. For the sake of easier implementation we apply a SWAP gate at the output of the QFT circuit, hence we are interested in



$$U_l \; : \quad |i_l\rangle \rightarrow |\mu_{n-l+1}\rangle$$

- Let us investigate first U_n.

$$i_n = 0, 1$$

$$e^{j2\pi 0.i_n} = \pm 1$$

$$\underbrace{\left(\frac{|0\rangle + e^{j2\pi 0.i_n}|1\rangle}{\sqrt{2}}\right)}_{|\mu_1\rangle}$$

$$|\mu_1\rangle = \begin{cases} \frac{|0\rangle + |1\rangle}{\sqrt{2}} & \text{if } i_n = 0 \\ \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{if } i_n = 1. \end{cases}$$

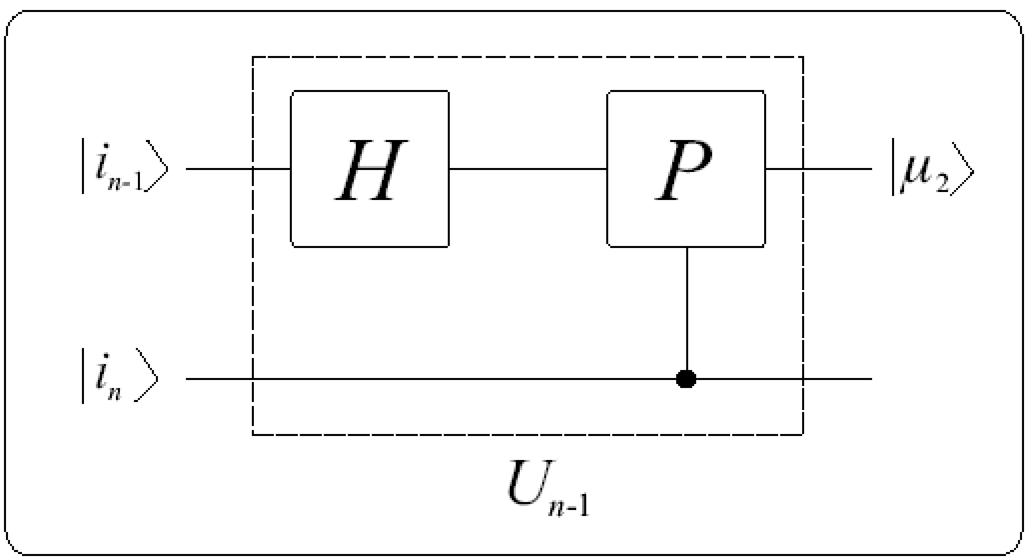
$$\boxed{U_n = H}$$

HOW TO IMPLEMENT QFT 5

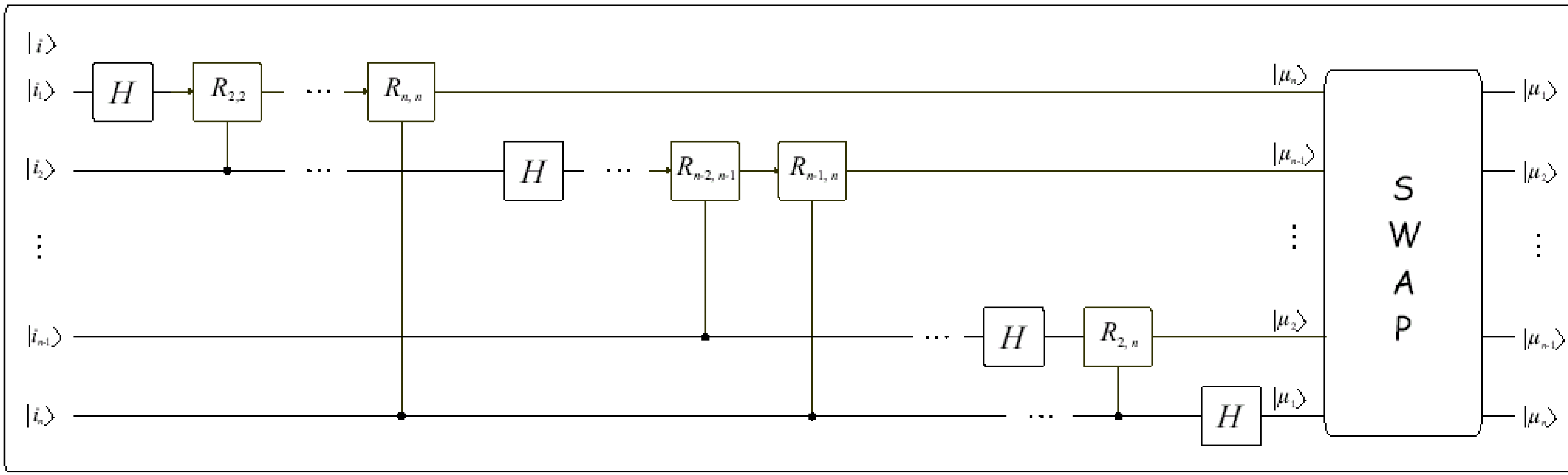
- Next we turn to $U_{n-1} : |i_{n-1}\rangle \rightarrow |\mu_2\rangle$

$$\underbrace{\left(\frac{|0\rangle + e^{j2\pi 0.i_{n-1}i_n}|1\rangle}{\sqrt{2}}\right)}_{|\mu_2\rangle}$$

$$|\mu_2\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle + e^{j2\pi 0.i_{n-1}} \cdot \left\{ \begin{array}{cc} P(2\pi\frac{1}{2^2})|1\rangle & \text{if } i_n = 1 \\ 1|1\rangle & \text{if } i_n = 0 \end{array} \right\}\right]$$

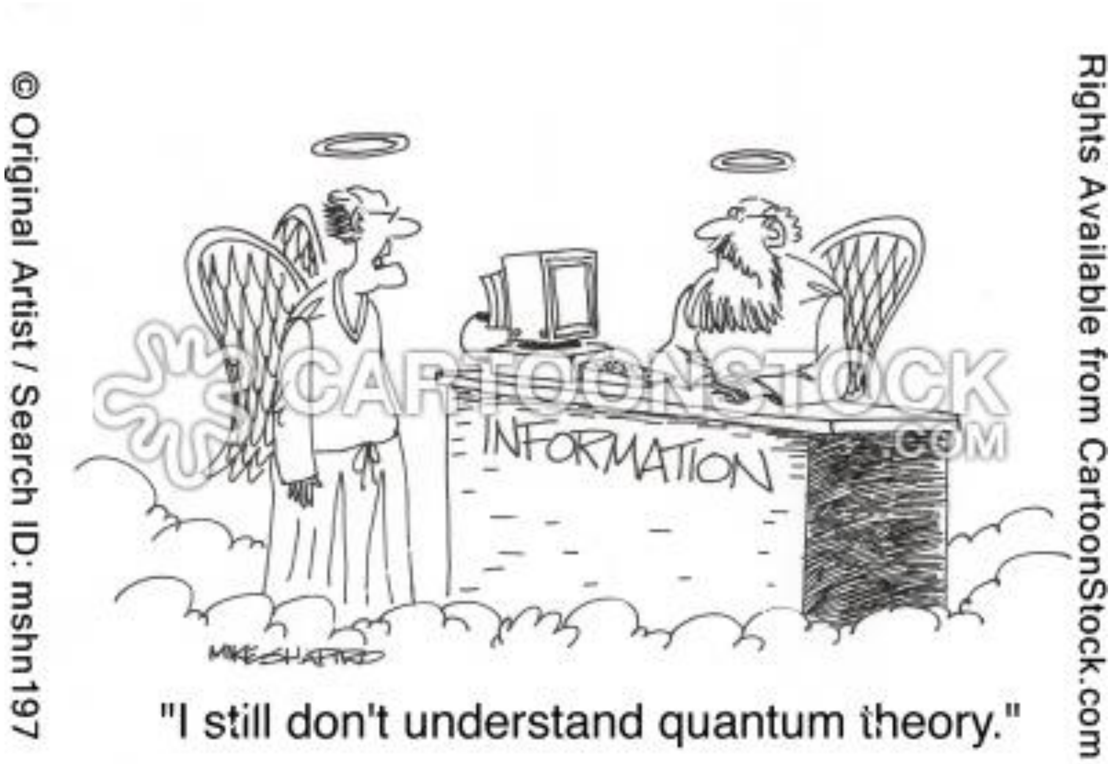


HOW TO IMPLEMENT QFT 6



$$R_{h,p} \triangleq \begin{cases} P(2\pi \frac{1}{2^h}) & \text{if } i_p = 1 \\ 1 & \text{if } i_p = 0 \end{cases}$$

- Remarks
  - Complexity: $O(n^2)$
  - QFT is not for computing Fourier coefficients in a faster way since they are represented by probability amplitudes!


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

DISCLAIMER

This presentation was presented as part of the Quantum Computing and its Application course @ Budapest University of Technology and Economics, Budapest, Hungary.
The course is offered by the Department of Networked Systems and Services (http://www.hit.bme.hu).

The development of this course material has received funding from the European Union under grant agreement No 101081247 (QCIHungary project) and has been implemented with the support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund.

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

QCIHungary