DEPARTMENT OF NETWORKED SYSTEMS AND SERVICES

Postulates

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

From the previous lecture

QUANTUM FLAGSHIP

Discover About Newsroom

Stay tuned

The future is Quantum.

The Second Quantum Revolution is unfolding now, exploiting the enormous advancements in our ability to detect and manipulate single quantum objects. The Quantum Flagship is driving this revolution in Europe.

LEARN MORE

unesco

INTERNATIONAL YEAR OF
Quantum Science
and Technology

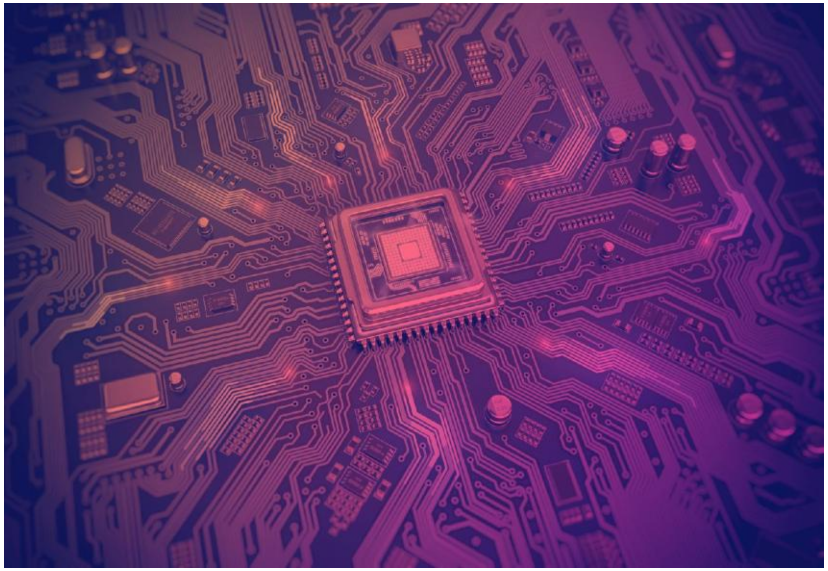
Home | About IYQ | Newsroom | Partners | Events | Get Involved

100 YEARS OF QUANTUM IS JUST THE BEGINNING

The 2025 International Year of Quantum Science and Technology (IYQ) recognizes 100 years since the initial development of quantum mechanics. Join us in engaging with quantum science and technology and celebrating throughout the year!

Search All Events →

WHAT DOES IT MEAN TO BE QUANTUM?



A system is quantum if it behaves according to the laws of quantum mechanics.

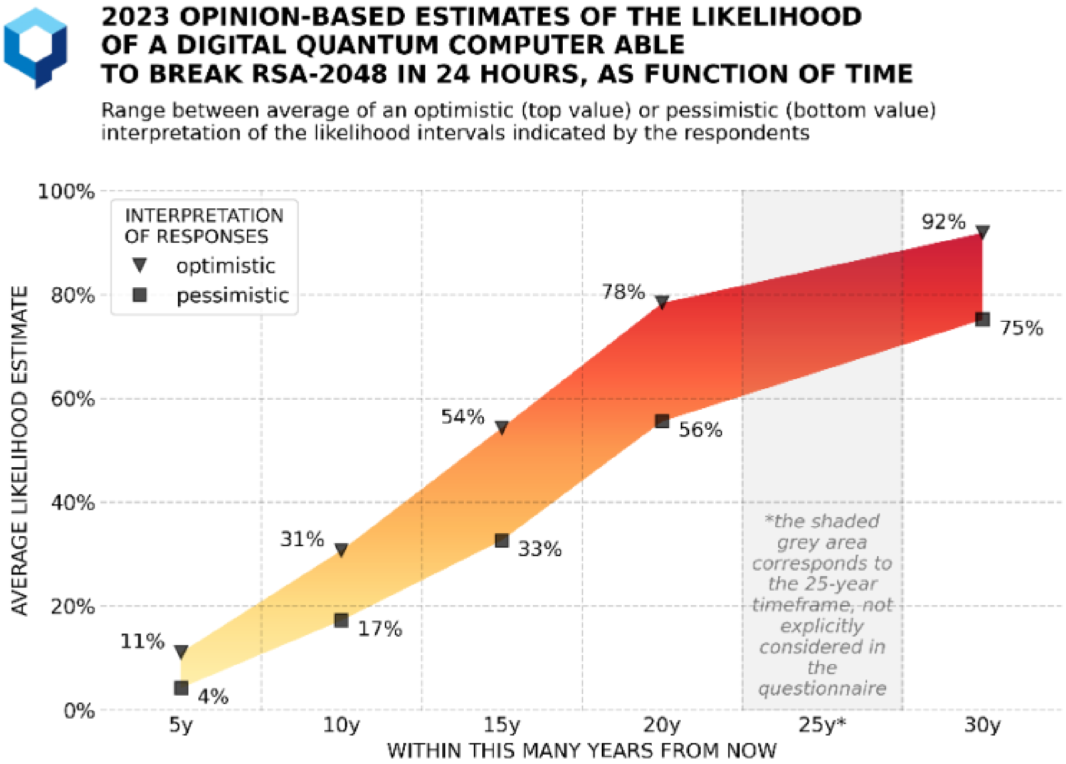
Quantum systems display peculiar features
- quantization
- wave-particle duality
- tunneling effects
- superposition
- quantum interference
- …

Quantum systems are typically microscopic

but

the laws of quantum mechanics are the basis of many macroscopic systems.

WHY NOW?



Forrás: Global Risk Institute 2023

Mosca inequality

Postulates

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

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

Quantum bits and quantum registers

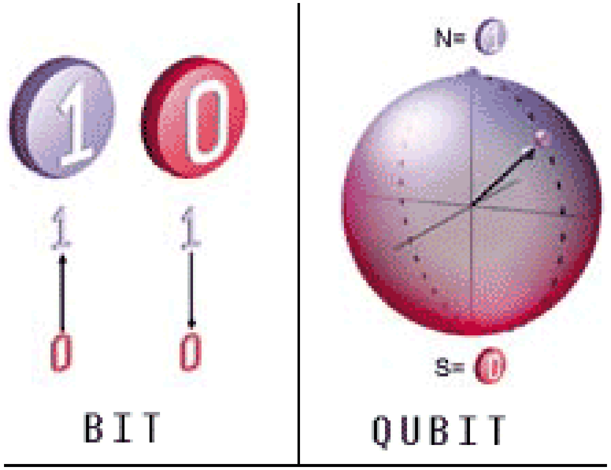
"All of the books in the world contain no more information than is broadcast as video in a single large American city in a single year. Not all bits have equal value."

Carl Sagan

1ST POSTULATE (STATE SPACE)

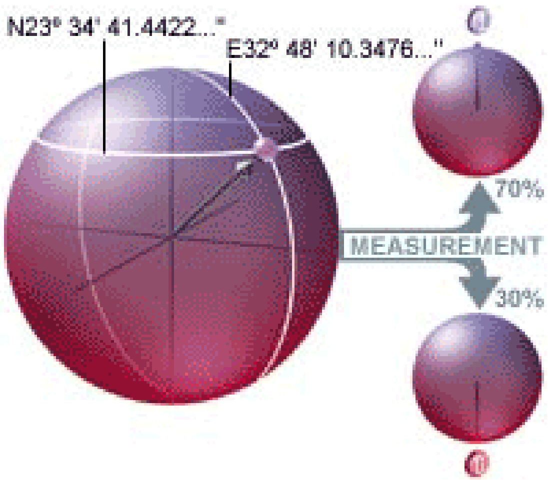
The actual state of any closed physical system can be described by means of a so called state vector **v** having complex coefficients and unit length in a Hilbert space *V* i.e. a complex linear vector space (state space) equipped with inner product.

QUANTUM BIT (QUBIT)



$$|\varphi\rangle = a|0\rangle + b|1\rangle$$

$$|a|^2 + |b|^2 = 1 \qquad a, b \in C$$



CLASSICAL BIT

0 or **1**

SUPERPOSITION

0 and **1**

SUPERPOSITION

QUANTUM BIT (QUBIT)

- Dirac's 'ket' and 'bra' notations: $|\varphi\rangle = (\langle\varphi|)^\dagger$
- Qubit: contains both classical states (computational basis states) at the same time in a so called superposition

$$|\varphi\rangle = a|0\rangle + b|1\rangle = a\begin{bmatrix}1\\0\end{bmatrix} + b\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}a\\b\end{bmatrix}$$

- where *a* and *b* are probability amplitudes. They squared absolute value carries the information about the probabilities of obtaining a certain classical states after measurement (in that classical basis)

$$|a|^2 + |b|^2 = 1$$

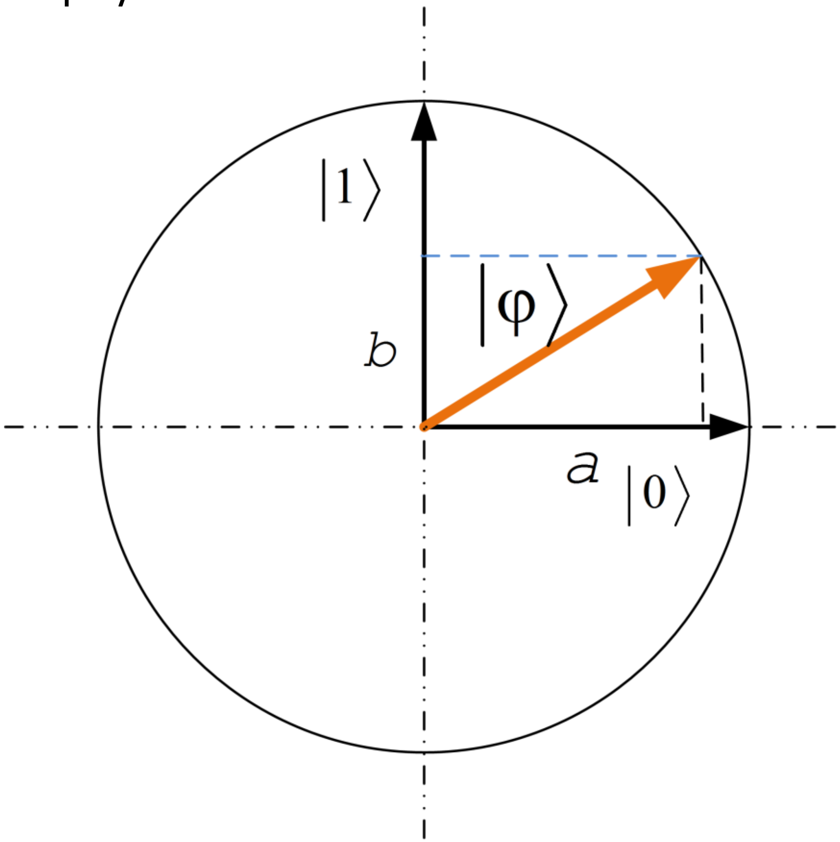
- Operations: inner and outer products

REPRESENTATION WITH REAL AMPLITUDES

$$\left|\varphi\right\rangle = a\left|0\right\rangle + b\left|1\right\rangle$$

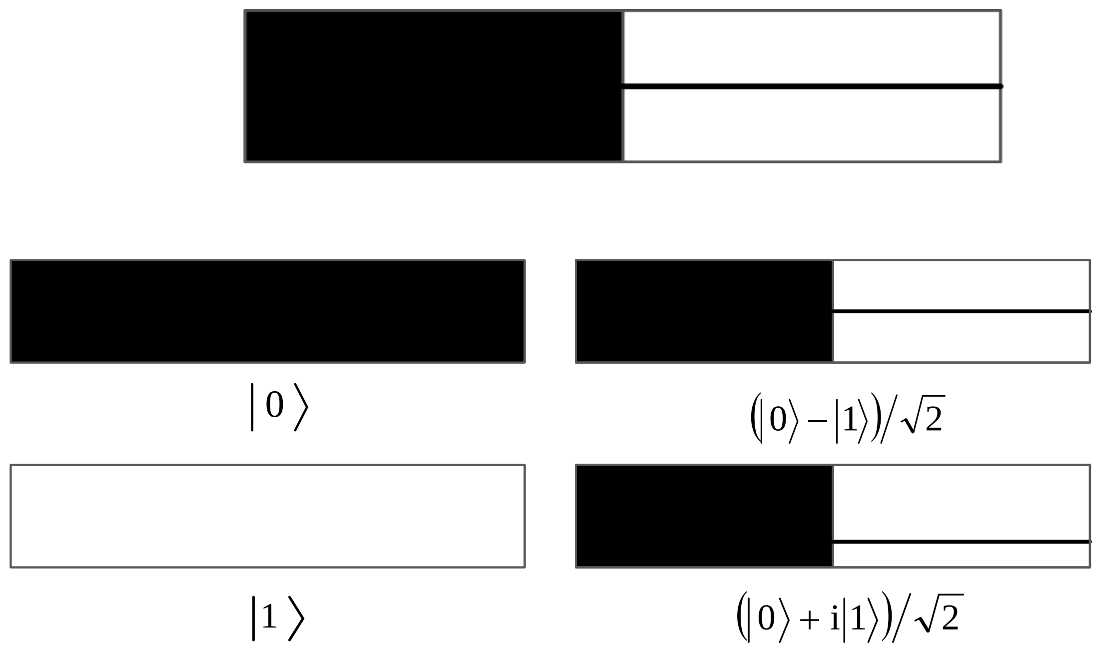
$$\left|a\right|^2 + \left|b\right|^2 = 1.$$

$$a, b \in C$$



L. Bacsardi, M. Galambos, S. Imre, A. Kiss. "Quantum Key Distribution over Space-Space Laser Communication Links," AIAA Space 2012, Pasadena, California, Sept, 2012.

REPRESENTATION WITH FRACTALS



M. Galambos, S. Imre, “Visualizing the Effects of Measurements and Logic Gates On Multi-Qubit Systems Using Fractal Representation,” *International Journal on Advances in Systems and Measurements,* Vol. 5, No. 1-2, 2012, pp. 1–10.

REPRESENTATION WITH BLOCH SPHERE

Bloch Sphere:

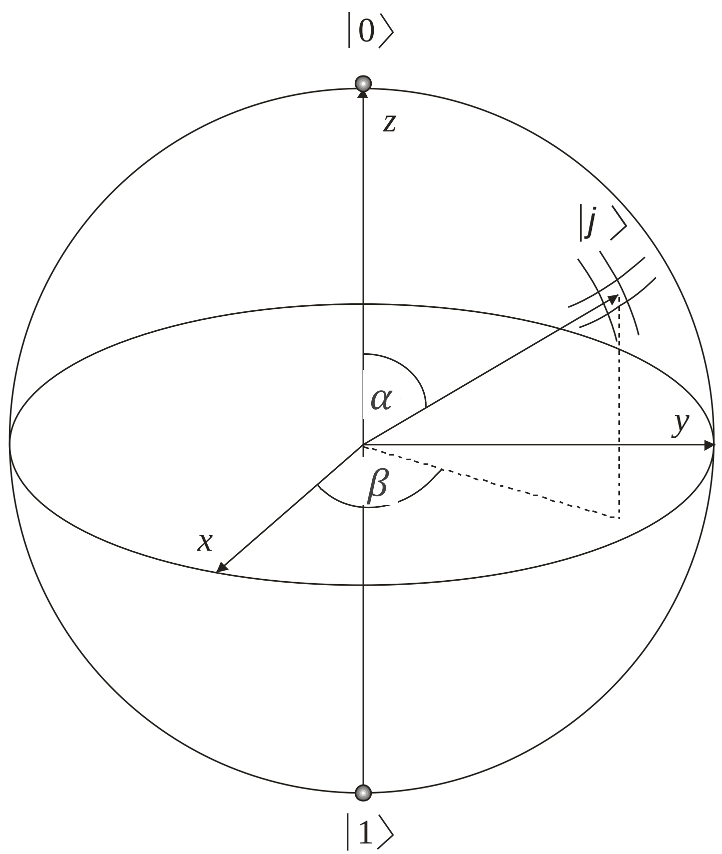
Visualizes a one-qubit system up to a certain global phase

$$|\varphi\rangle = e^{j\gamma}\left[\cos\left(\frac{\alpha}{2}\right)|0\rangle + e^{j\beta}\sin\left(\frac{\alpha}{2}\right)|1\rangle\right] \quad \alpha, \beta, \gamma \in \mathbb{R}$$

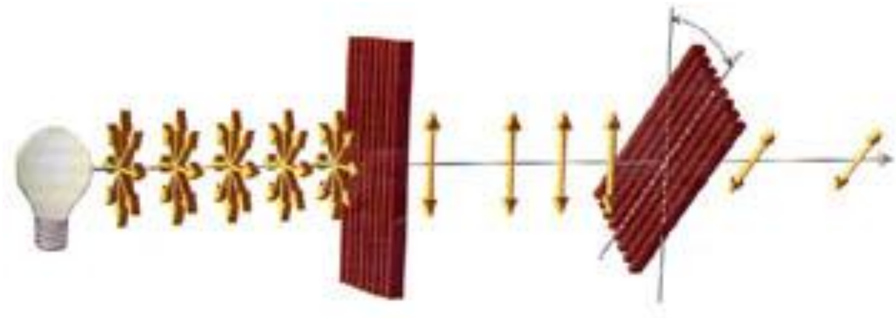
$$|\varphi\rangle = [x, y, z]^T = [\cos(\beta)\sin(\alpha), \sin(\beta)\sin(\alpha), \cos(\alpha)]^T$$

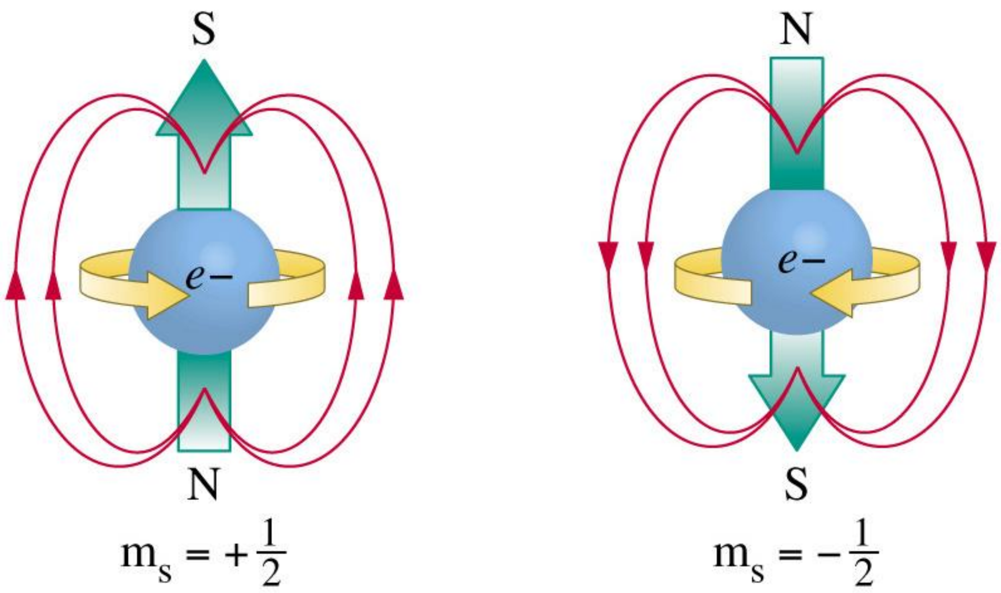
BLOCH SPHERE

$$|\varphi\rangle = e^{j\gamma}\left[\cos\left(\frac{\alpha}{2}\right)|0\rangle + e^{j\beta}\sin\left(\frac{\alpha}{2}\right)|1\rangle\right] \quad \alpha,\beta,\gamma \in \mathbb{R}$$



QUANTUM BITS IN PRACTICE





REMARKS

- We strongly emphasize here again that before the measurement the qubit has both logical values, i.e., it is in both computational basis states at the same time
- and the measurement let the qubit collapse into one of them. This completely differs from the classical approach which assumes that the coin is in one of the logical states before the measurement and the measurement only reveals this fact.

4TH POSTULATE (COMPOSITE SYSTEMS)

- The state space of a composite physical system W can be determined using the tensor product of the individual systems $W = V \otimes Y$. Furthermore having defined $\mathbf{v} \in V$ and $\mathbf{y} \in Y$ then the joint state of the composite system is $\mathbf{w} = \mathbf{v} \otimes \mathbf{y}$.

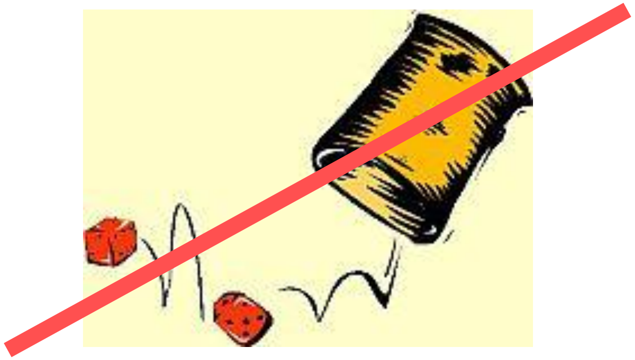
WHAT IS 500 QUBIT GOOD FOR?

Quantum register 500 qubits of length contains more numbers in a superposition than the number of atoms in the universe…

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

NATURE OF NATURE

God does not play dice with the universe



But it does!

MERGING QUBITS TO QUREGISTERS

Two-qubit example of 4th Postulate

$$|\varphi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, |\varphi_2\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$\begin{aligned} |\varphi\rangle &\equiv |\varphi_1\rangle|\varphi_2\rangle \equiv |\varphi_1, \varphi_2\rangle \equiv |\varphi_1\varphi_2\rangle \\ &= \frac{|0\rangle \otimes |0\rangle + |1\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle + |1\rangle \otimes |1\rangle}{2} = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2} \end{aligned}$$

$$|\varphi_1\rangle = |0\rangle \quad |\varphi_2\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|\varphi\rangle = |0\rangle \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{|00\rangle + |01\rangle}{\sqrt{2}}$$

General case:

n-qubit register

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

QUANTUM REGISTERS

$$|\varphi\rangle = a|0\rangle + b|1\rangle$$

$$|\varphi\rangle^{\otimes 2} = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

$$|\varphi\rangle^{\otimes 4} = a|0000\rangle + b|0001\rangle + \ldots + o|1110\rangle + p|1111\rangle$$

QUREGISTER

Elementary gates

""Excellent!" I cried,

"Elementary" said he.

Watson and Holmes, in "The Crooked Man", The Memoirs of Sherlock Holmes,

Sir Arthur Conan Doyle

2ND POSTULATE (EVOLUTION)

- The evolution of any closed physical system in time can be characterized by means of unitary transforms depending only on the starting and finishing time of the evolution.

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

- The above definition describes the evolution between discrete time instants, which is more suitable in context of quantum computing. Its original continuous-time form is known as Schrödinger equation

$$H\mathbf{v} = i\hbar\frac{\partial \mathbf{v}}{\partial t}$$

- Relationship between *H* and *U*

$$U(t_1, t_2) = e^{\frac{-iH(t_2 - t_1)}{\hbar}}$$

PARADOX OF AND GATE

- Unitary transforms: reversible distance-preserving maps.
- Classical AND, XOR etc. gates are irreversible.
- This seems to be a paradox since classical world can be regarded as part of quantum one.

PAULI GATES

$$|\varphi\rangle = a|0\rangle + b|1\rangle$$

- Pauli X (bit-flip) gate:

$$\begin{bmatrix} a \\ b \end{bmatrix}$$

$$|\psi\rangle = X|\varphi\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} b \\ a \end{bmatrix} = b|0\rangle + a|1\rangle$$

- Pauli *Z* (phase-flip) gate:

$$\begin{bmatrix} a \\ b \end{bmatrix}$$

$$|\psi\rangle = Z|\varphi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} a \\ -b \end{bmatrix} = a|0\rangle - b|1\rangle$$

PAULI GATES (2)

$$|\varphi\rangle = a|0\rangle + b|1\rangle$$

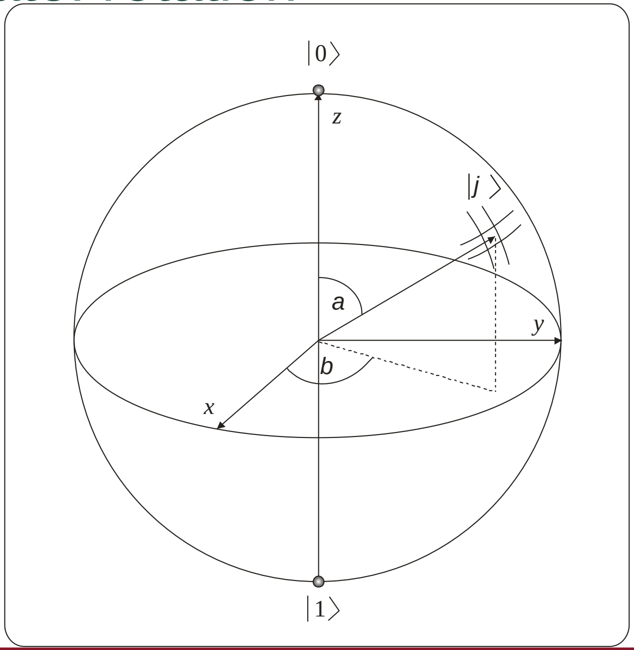
- Pauli *Y* (double-flip) gate:

$$\begin{bmatrix} a \\ b \end{bmatrix}$$

$$|\psi\rangle = Y|\varphi\rangle = \begin{bmatrix} 0 & -j \\ j & 0 \end{bmatrix} \begin{bmatrix} -jb \\ ja \end{bmatrix} = -jb|0\rangle + ja|1\rangle$$

- Geometrical interpretation of Pauli *X* gate: rotation around axis *x* in the Bloch sphere

$$e^{-j\frac{\alpha}{2}X} = \cos\left(\frac{\alpha}{2}\right) I - j\sin\left(\frac{\alpha}{2}\right) X$$



PHASE GATE

$|\varphi\rangle = a|0\rangle + b|1\rangle$

- Phase gate:

$$\begin{bmatrix} a \\ b \end{bmatrix}$$

$$|\psi\rangle = P(\alpha)|\varphi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{j\alpha} \end{bmatrix} \begin{bmatrix} a \\ e^{j\alpha} b \end{bmatrix} = a|0\rangle + e^{j\alpha} b|1\rangle$$

HADAMARD GATE

$$|\varphi\rangle = a|0\rangle + b|1\rangle$$

$$\begin{bmatrix} a \\ b \end{bmatrix}$$

$$|\psi\rangle = H|\varphi\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} \frac{a+b}{\sqrt{2}} \\ \frac{a-b}{\sqrt{2}} \end{bmatrix} = \frac{a+b}{\sqrt{2}}|0\rangle + \frac{a-b}{\sqrt{2}}|1\rangle$$

- Hadamard gate is Hermitian i.e. $H^\dagger = H$
- furthermore: $HH = I$
- *H* gate prepares uniform superposition: $$\boxed{\begin{aligned} H|0\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \\ H|1\rangle &= \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \end{aligned}}$$

HADAMARD GATE

- n-qubit Hadamard gate whit input $|\varphi\rangle = |000...0\rangle$

$$|\psi\rangle = H^{\otimes n}|\varphi\rangle = \frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}|i\rangle$$

- n-qubit Hadamard gate with arbitrary classical input

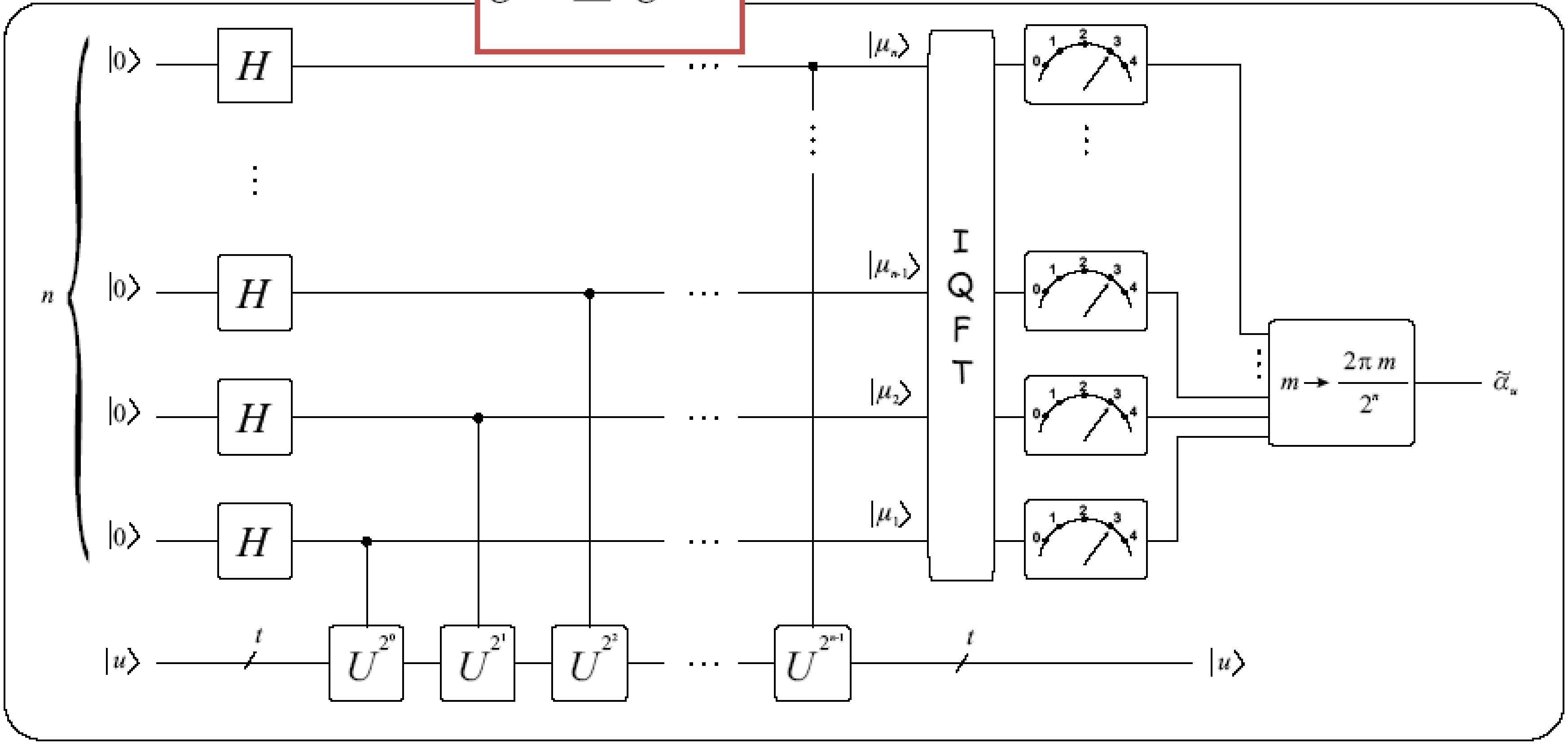
$$k = 0, 1, ...2^n - 1$$

$$H^{\otimes n}|k\rangle = \frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}(-1)^{ik}|i\rangle$$

QUANTUM GATES

A quantum gate operates on each element of the input superposition and gives a modified superposition back at its output.

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



Measurement

Cannon balls: a quantum mechanical treatment.

3RD POSTULATE (MEASUREMENT)

- Any quantum measurement can be described by means of a set of measurement operators $\{M_m\}$, where *m* stands for the possible results of the measurement. The probability of measuring m if the system is in state **v** can be calculated as

$$P(m \mid \mathbf{v}) = \mathbf{v}^\dagger M_m^\dagger M_m \mathbf{v}$$

- and the system after measuring m gets in state

$$\mathbf{v}' = \frac{M_m \mathbf{v}}{\sqrt{\mathbf{v}^\dagger M_m^\dagger M_m \mathbf{v}}}$$

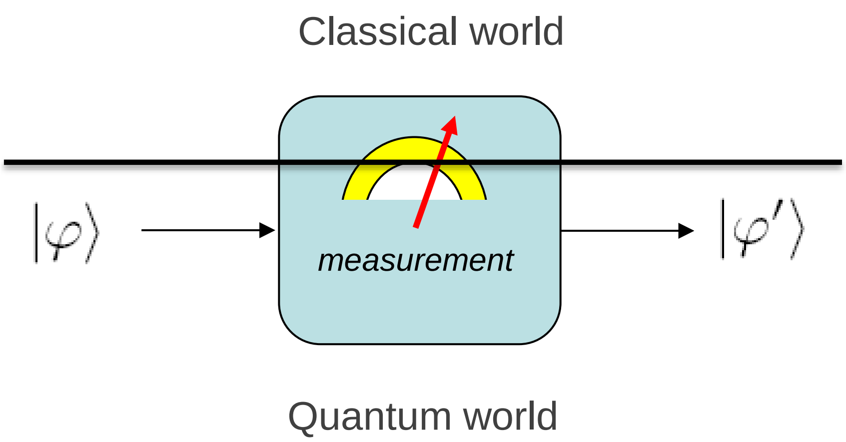
- Because classical probability theory requires that

$$\sum_m P(m \mid \mathbf{v}) = \sum_m \mathbf{v}^\dagger M_m^\dagger M_m \mathbf{v} \equiv 1$$

- *Completeness relation:* $\boxed{\sum_m M_m^\dagger M_m \equiv I}$

3RD POSTULATE (MEASUREMENT)

- Projects quantum superpositions to one of its elements with certain probability.
- It gives a classical value back.



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

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

Postulates

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

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

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