

QUANTUM WONDERS

Artur Ekert



Quanta, randomness, ciphers and computers...

- **Few random thoughts about the history of randomness**
- **Kolmogorov, his axioms and our nonconforming quantum world**
- **Quantum interference is all you should remember from this lecture**
- **Impossible quantum logic gates**
- **Quantum computers, their power and vulnerabilities**
- **When will Google, Baidu or John Doe build a quantum computer?**

Artur Ekert

Mathematical Institute, University of Oxford
CQT, National University of Singapore
OIST

Randomness – objective or subjective?

EPICURUS
(300 BC)

DEMOCRITUS
(400 BC)

atoms *swerve* at
random along
their paths

atoms follow
predetermined paths

SUBJECTIVE

Determinism, free will & moral responsibility



The Last Judgement, Hieronymus Bosch (1482)

Measure – early intuition about averages



Determination of the rod, using the length of the left foot of 16 randomly chosen people coming from church service. Woodcut published in the book *Geometrei* by [Jakob Köbel](#) c. 1535

More pragmatic approach - gambling



Caravaggio, The Cardsharps c. 1594

Girolamo Cardano - Gambling Scholar



1501-1576

Cardano described himself as

Hot-tempered, single-minded, and given to women, ...cunning, crafty, sarcastic, diligent, impertinent, sad, treacherous, magician and sorcerer, miserable, hateful, lascivious, obscene, lying, obsequious,...fond of the prattle of old men.

Enter complex numbers

10. quare nos volumus quadruplum totius
a b, igitur fiat a d, quadratum a c, dimidiū
a b, & ex a d auferatur quadruplum a b,
absque numero, R. igitur residui, si aliquid
maneret, addita & detracta ex a c, ostende-
ret partes, at quia tale residuum est minus,
ideo imaginaberis R. m. 15. id est differen-
tiæ a d, & quadrupli a b, quam adde &
minue ex a c, & habebis quæsitum, scili-
cet 5. p. R. v. 25. m. 40. & 5. m. R. v. 25.
m. 40. seu 5. p. R. m. 15. & 5. m. R. m.
15. duc 5. p. R. m. 15. in 5. m. R. m. 15.
dimissis incruciationibus, fit 25. m. m. 15.
quod est p. 15. igitur hoc productum est
40. natura tamen a d, non est eadem cum
natura 40. nec a b, quia superficies est

5. p. R. m. 15.

5 m. R. m. 15.

25. m. m. 15. quad. est 40.

Find two numbers
which sum to 10
and their product is 40

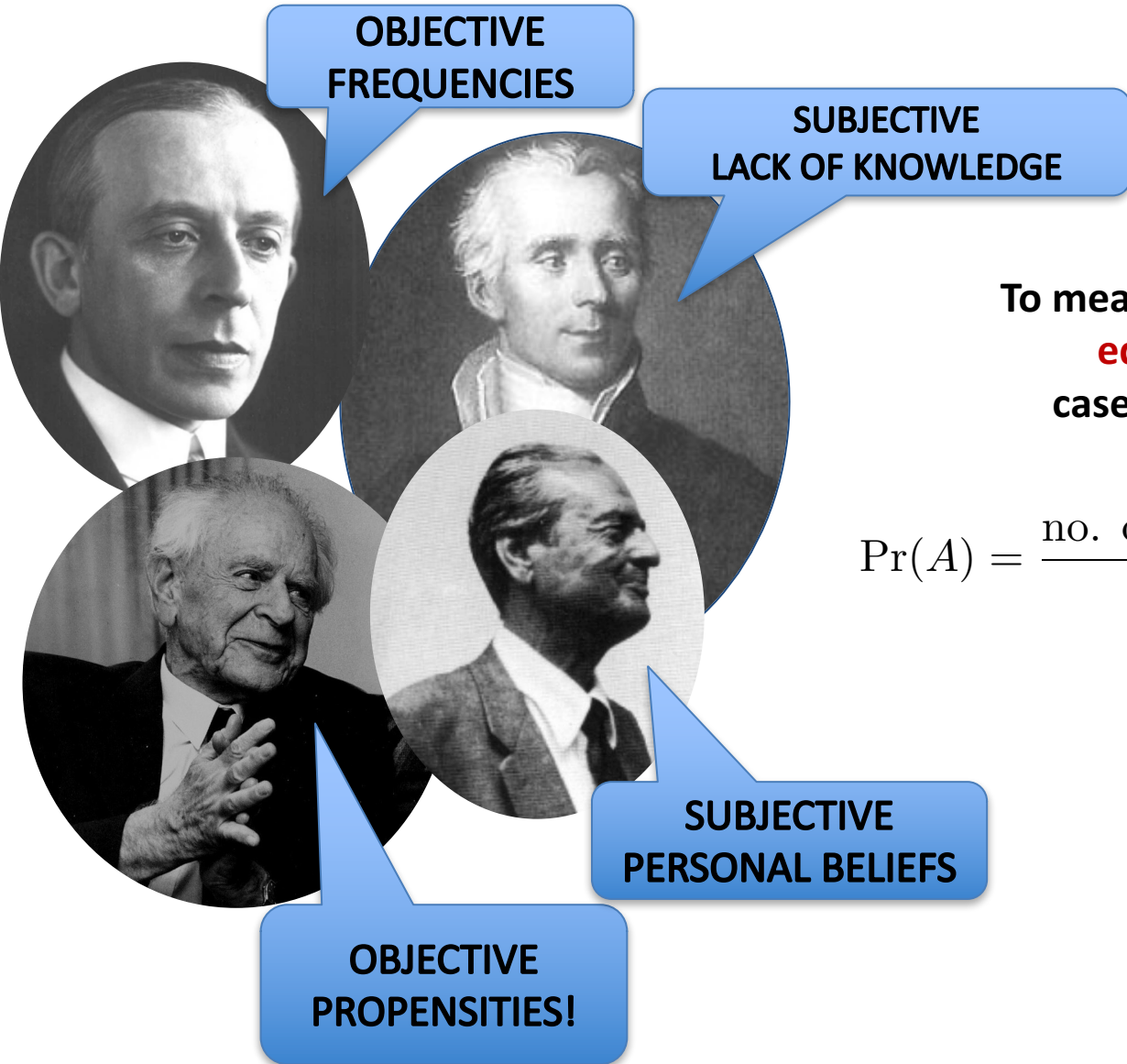
$$(5 + \sqrt{-15})(5 - \sqrt{-15})$$

$$25 - (-15)$$

$$25 + 15$$

$$40$$

What is probability...



OBJECTIVE
FREQUENCIES

SUBJECTIVE
LACK OF KNOWLEDGE

To measure probability find
equally probable
cases and count them

$$\Pr(A) = \frac{\text{no. of cases in which } A \text{ occurs}}{\text{total no. of cases}}$$

SUBJECTIVE
PERSONAL BELIEFS

OBJECTIVE
PROPENSITIES!

And then came Kolmogorov...

ERGEBNISSE DER MATHEMATIK
UND IHRER GRENZGEBIETE
HERAUSGEGEBEN VON DER SCHRIFTFLEITUNG
DES
„ZENTRALBLATT FÜR MATHEMATIK“
ZWEITER BAND

3

GRUNDBEGRIFFE DER WAHRSCHEINLICHKEITS- RECHNUNG

VON
A. KOLMOGOROFF

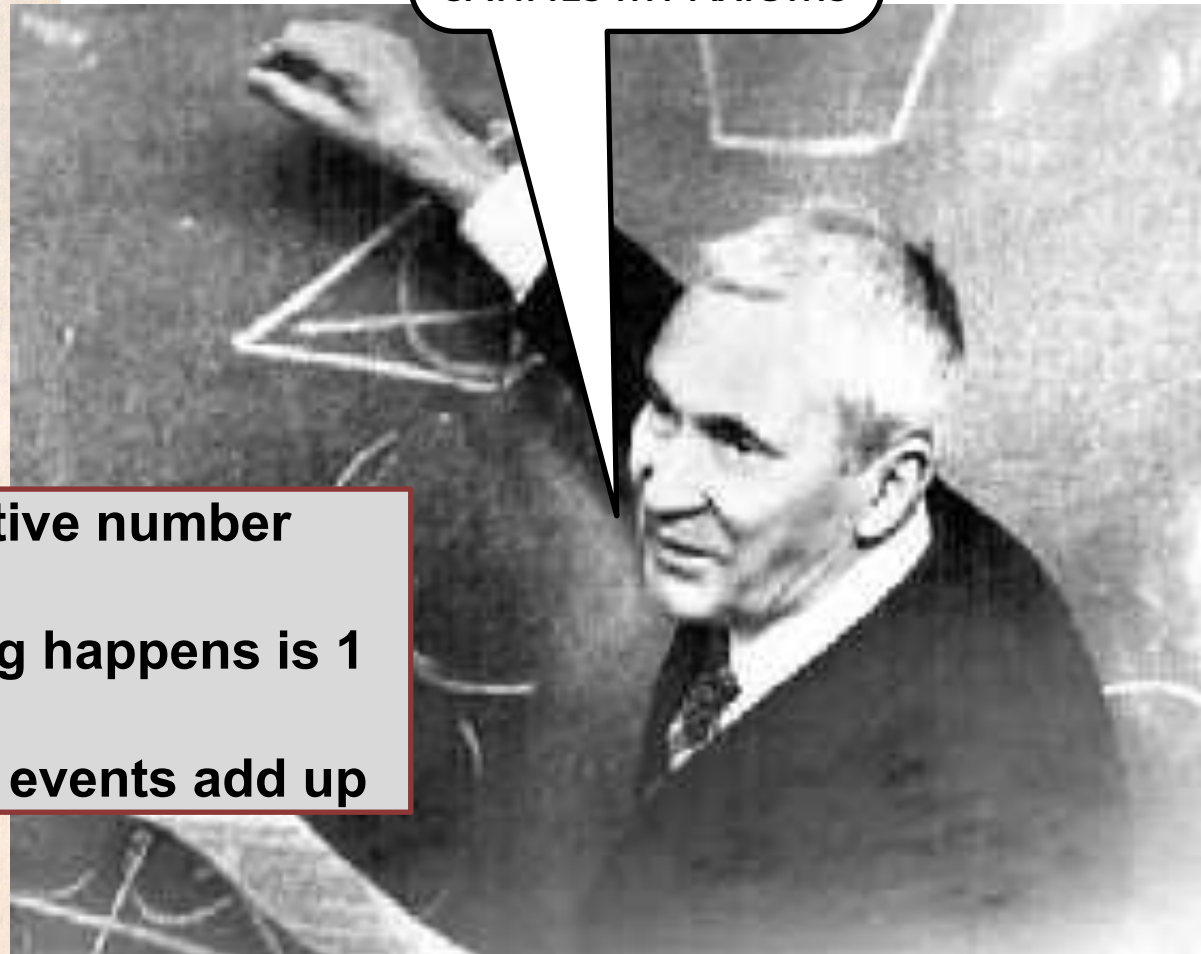
Probability is a non-negative number

Probability that something happens is 1

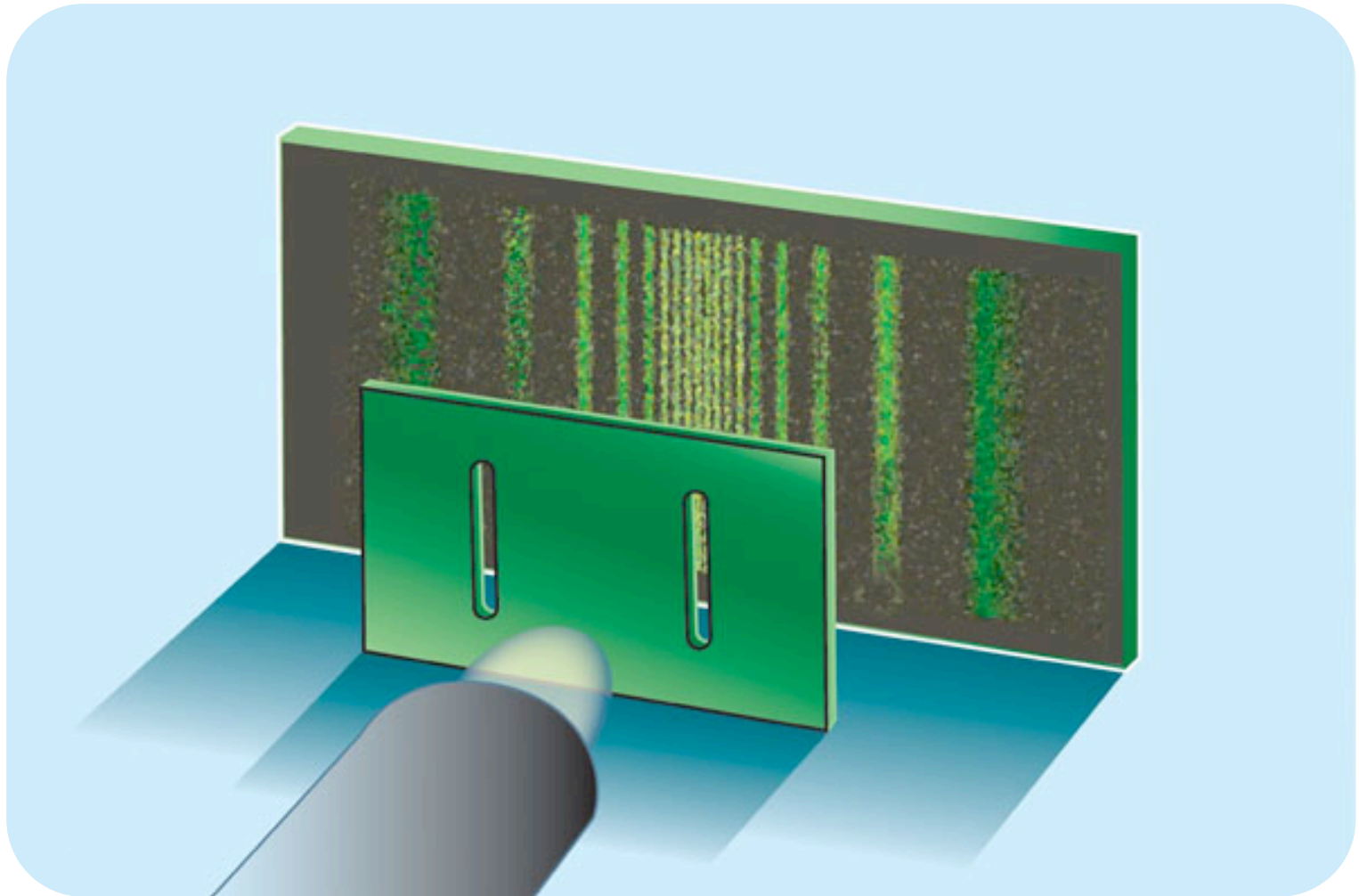
Probabilities of exclusive events add up

BERLIN
VERLAG VON JULIUS SPRINGER
1933

**I DON'T CARE!
PROBABILITY IS
ANYTHING THAT
SATISFIES MY AXIOMS**

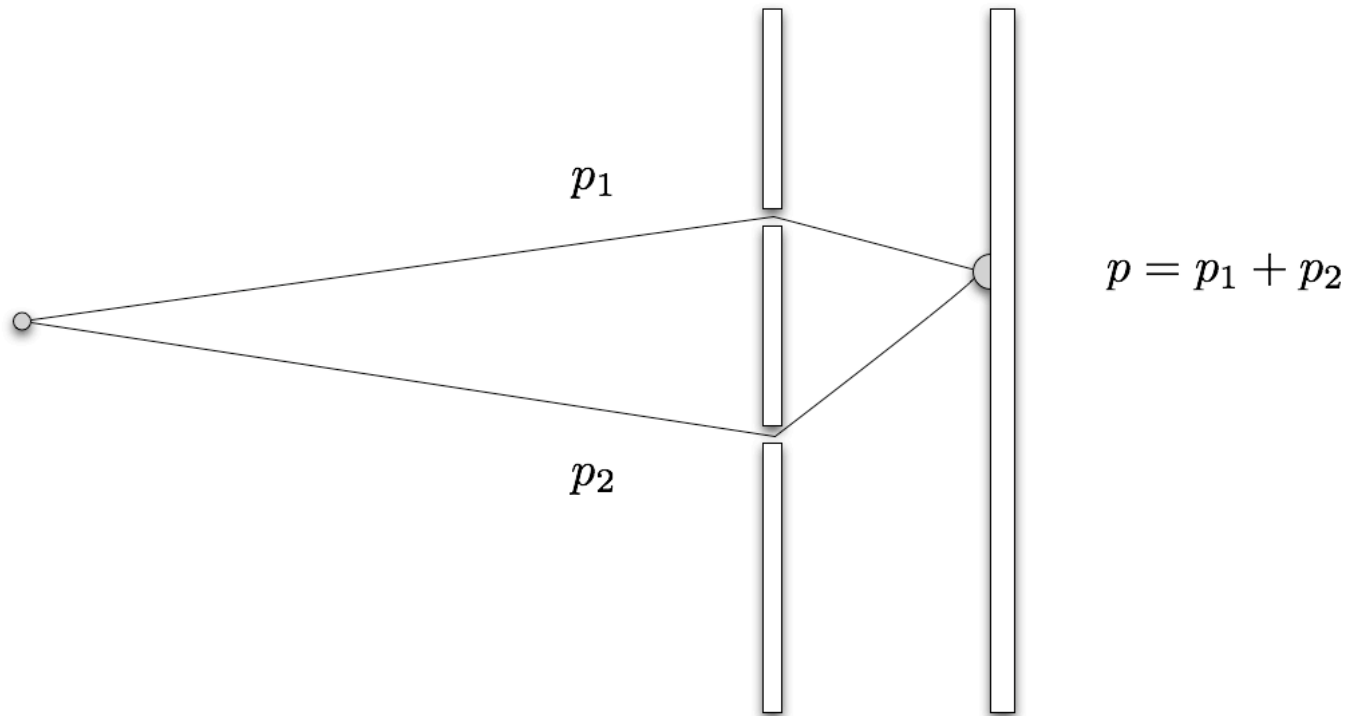


It's all very well, except that...



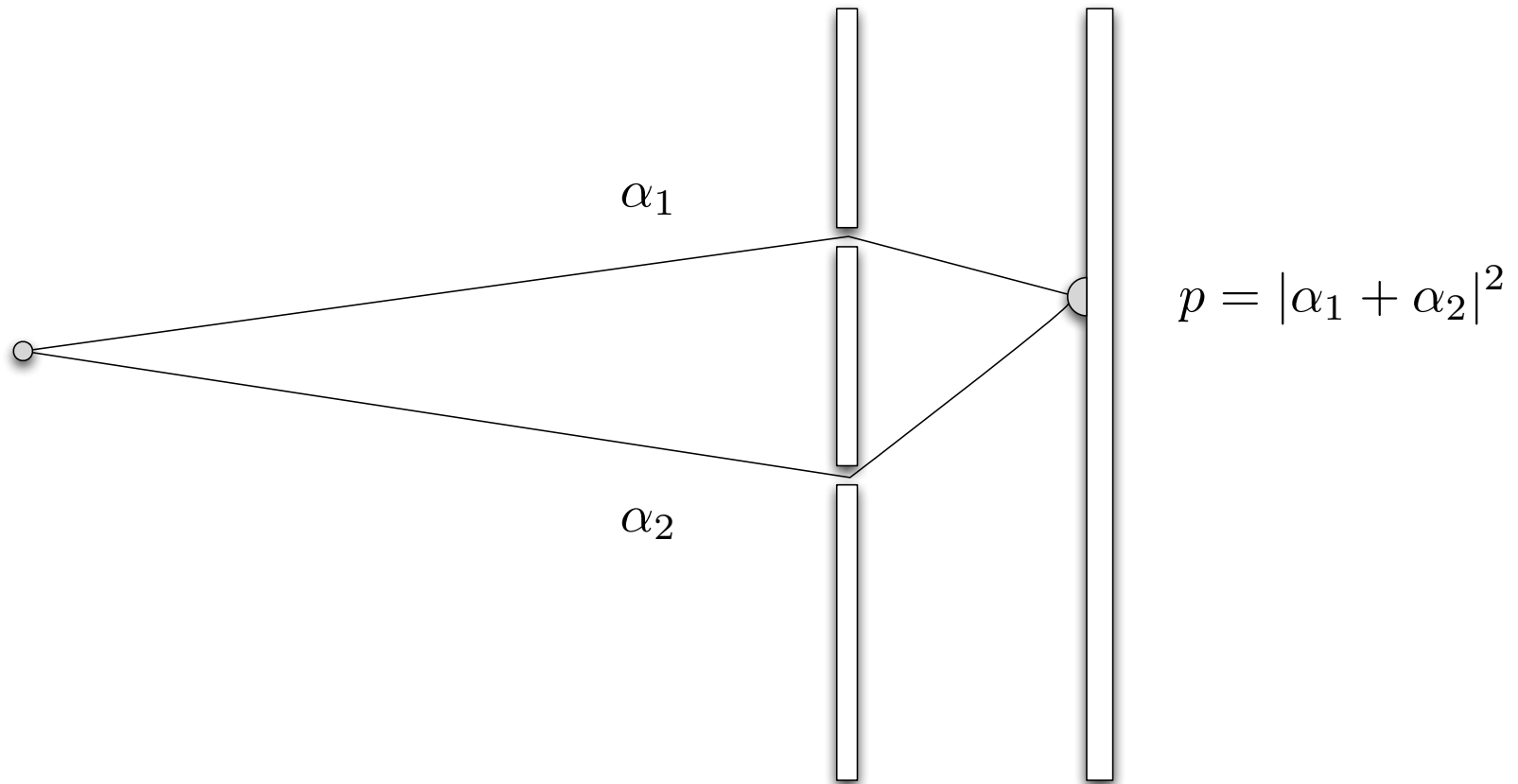
...Nature ignores additivity axiom

Whenever an event can occur in several mutually exclusive ways, the probability for the event is the sum of the probabilities for each way considered separately.

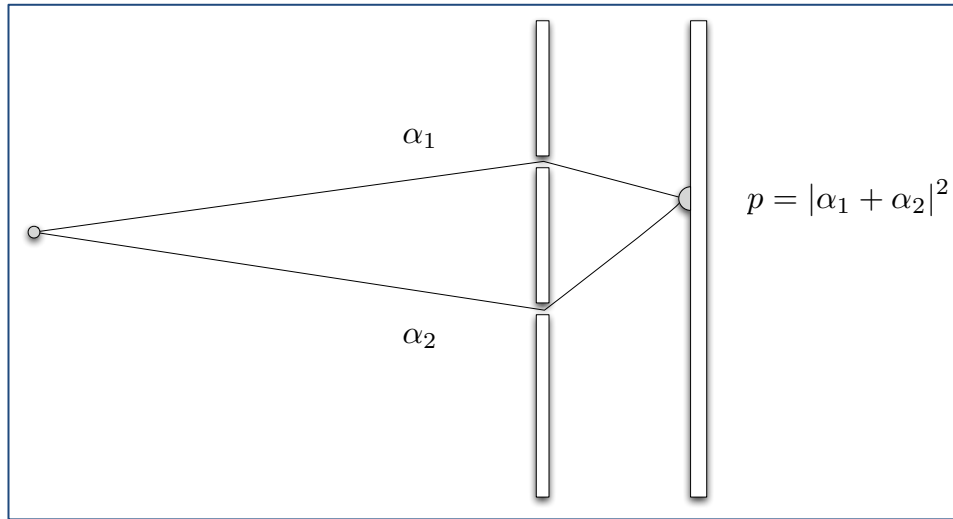


Additivity axiom revisited

Whenever an event can occur in several mutually exclusive ways, the **probability amplitude** for the event is the sum of the **probability amplitudes** for each way considered separately.



Quantum interference



$$\alpha_1 = |\alpha_1| e^{i\varphi_1}$$

$$\alpha_2 = |\alpha_2| e^{i\varphi_2}$$

$$\begin{aligned} |\alpha_1 + \alpha_2|^2 &= |\alpha_1|^2 + |\alpha_2|^2 + \alpha_1 \alpha_2^* + \alpha_1^* \alpha_2 \\ &= p_1 + p_2 + 2|\alpha_1||\alpha_2| \cos(\varphi_1 - \varphi_2) \end{aligned}$$

$$p = p_1 + p_2 + 2\sqrt{p_1 p_2} \cos(\varphi_1 - \varphi_2)$$

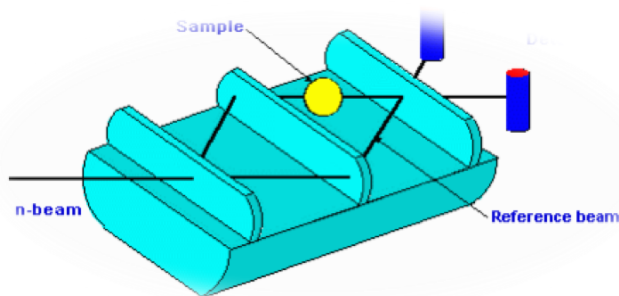
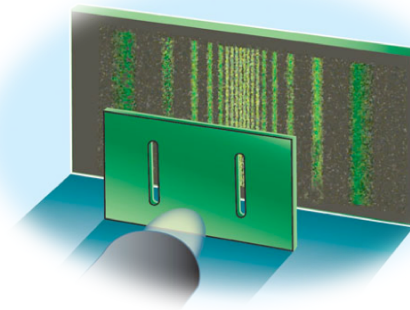
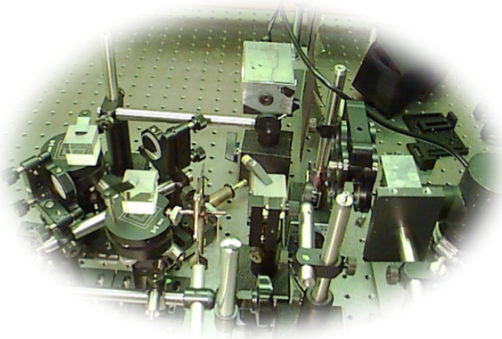
Quantum world is somewhat different...



©Charles Addams

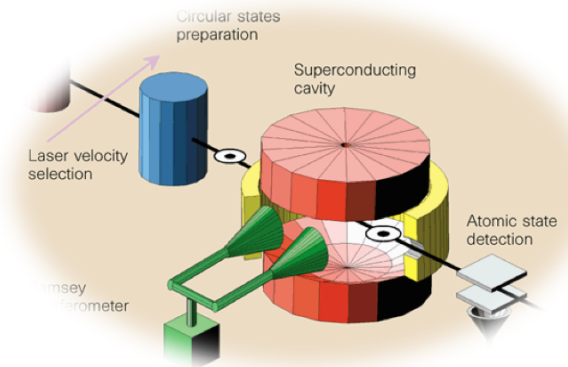
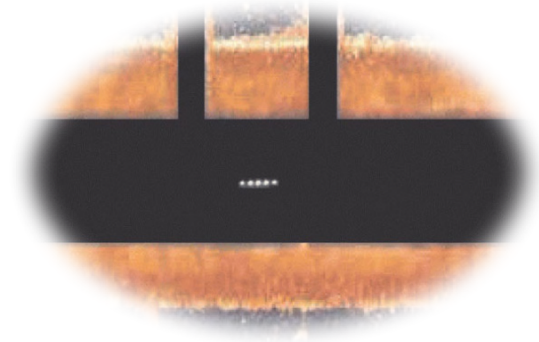
Ubiquitous quantum interference

PHOTONS



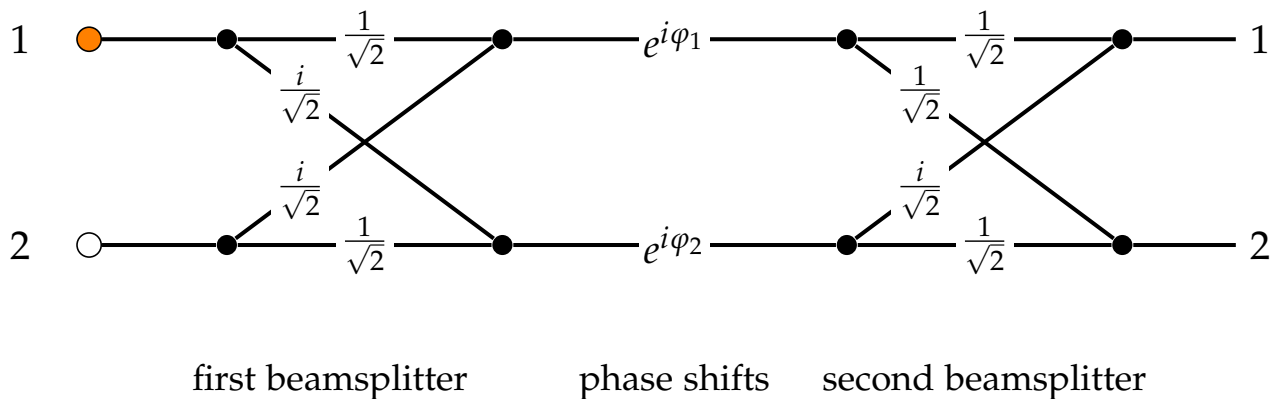
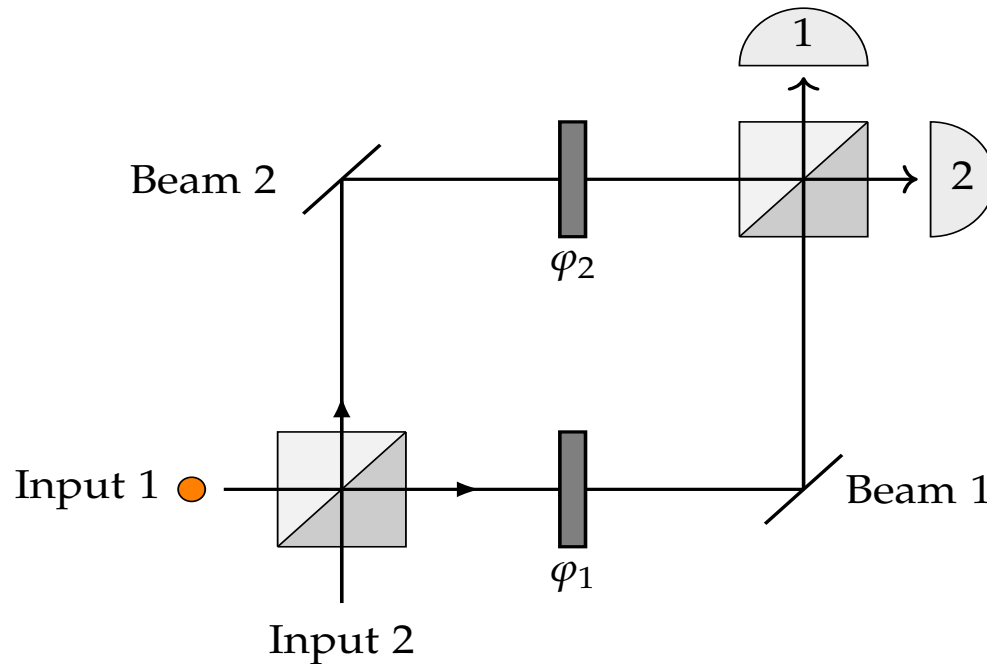
NEUTRONS

IONS

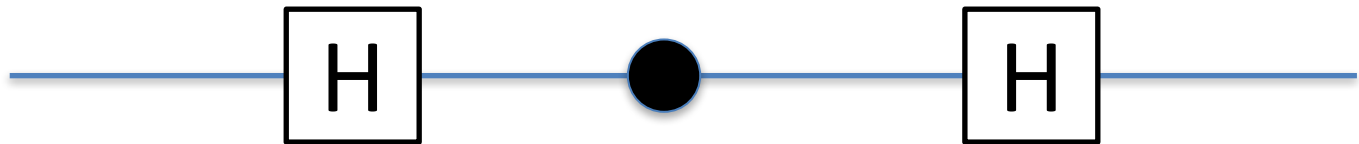
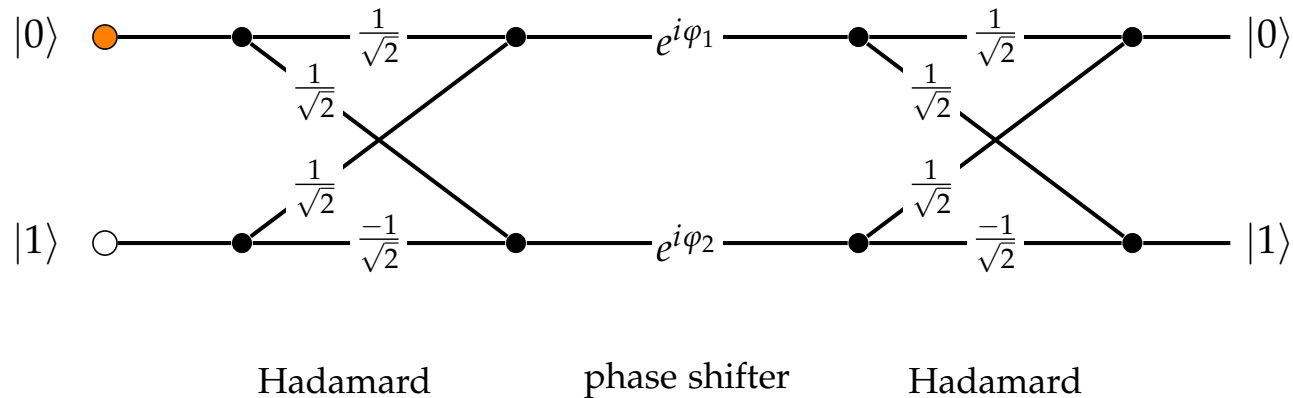


ATOMS

Mach-Zehnder interferometer

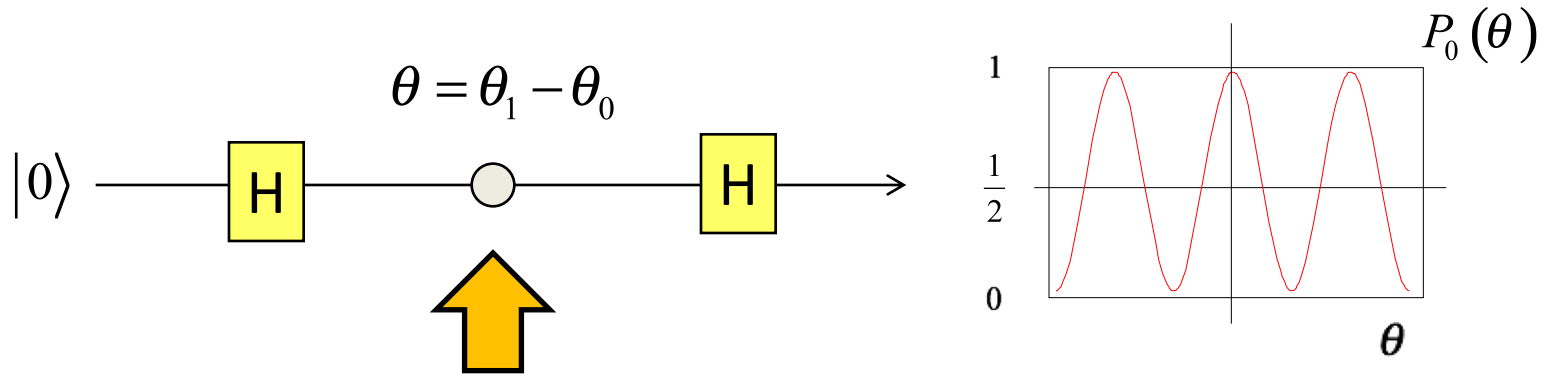


In terms of gates and circuits...



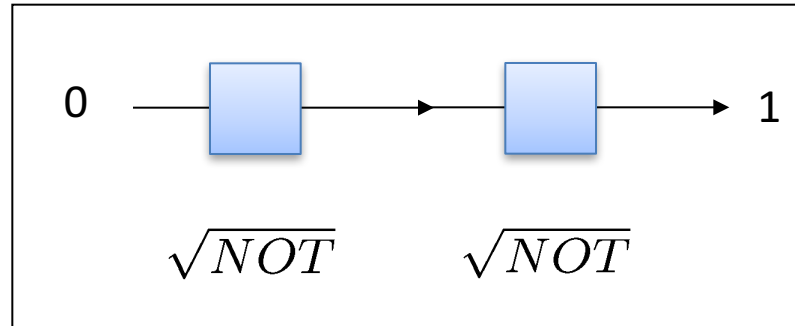
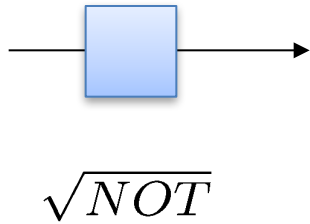
$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} e^{i\varphi_0} & 0 \\ 0 & e^{i\varphi_1} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix}$$

Quantum gravimeters, acelerometers

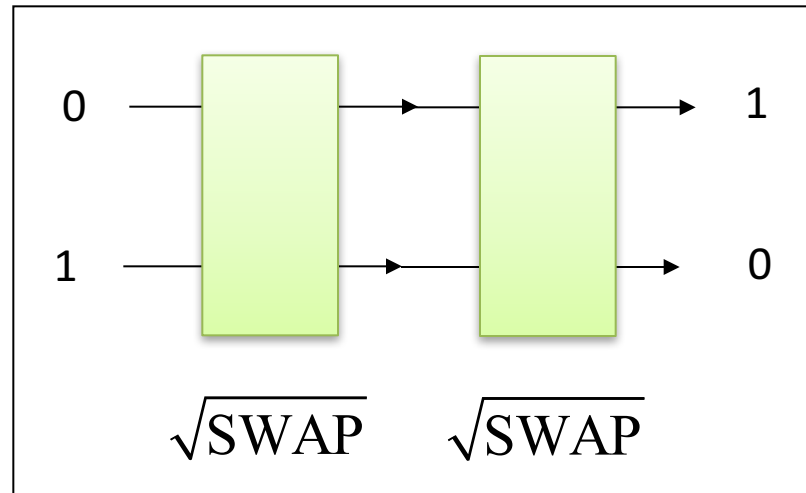
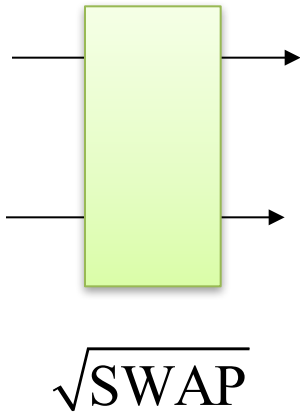


- Accelerations
- Rotations
- Laser frequency detuning
- Laser phase
- Photon recoil
- Electric/magnetic fields
- Interactions with atoms and molecules

Logically impossible gates



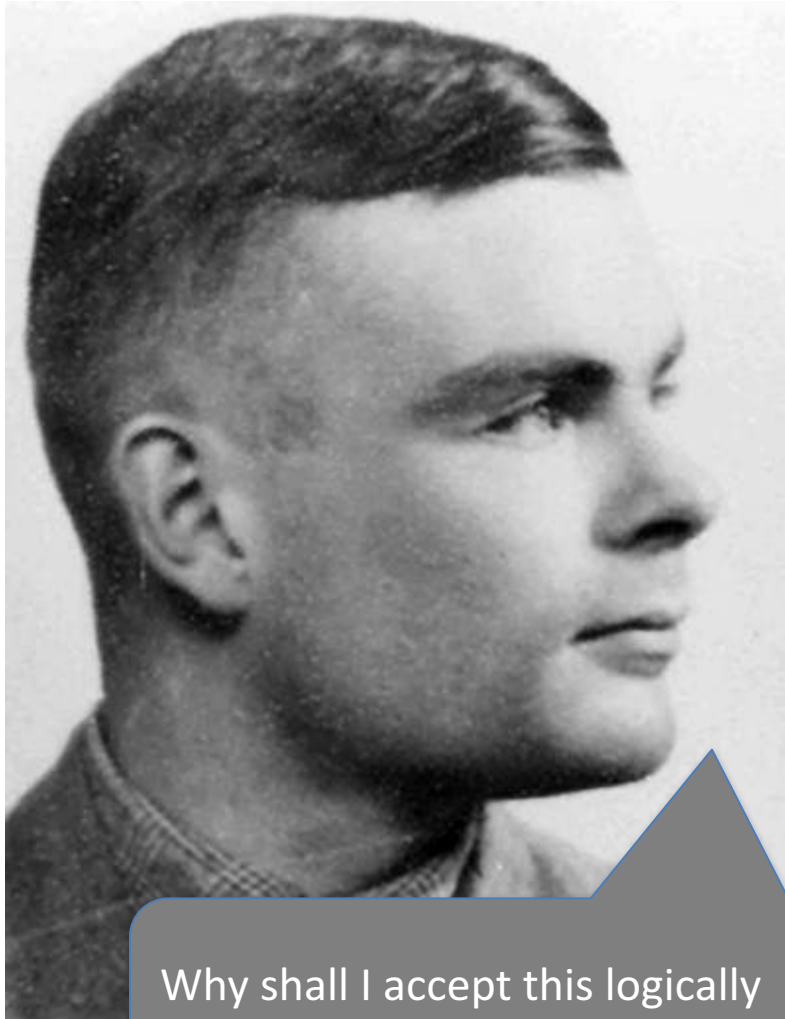
NOT



SWAP

Limits to computation ?

Alan Turing



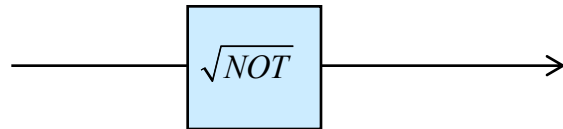
Why shall I accept this logically impossible operation \vee NOT ?

Because its physical representation exists in Nature. It can be performed!



David Deutsch

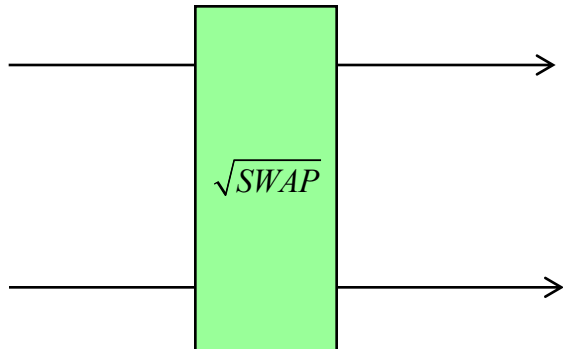
This is all we need...



$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$$

Generates superpositions

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



$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} & 0 \\ 0 & \frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Generates entanglement

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



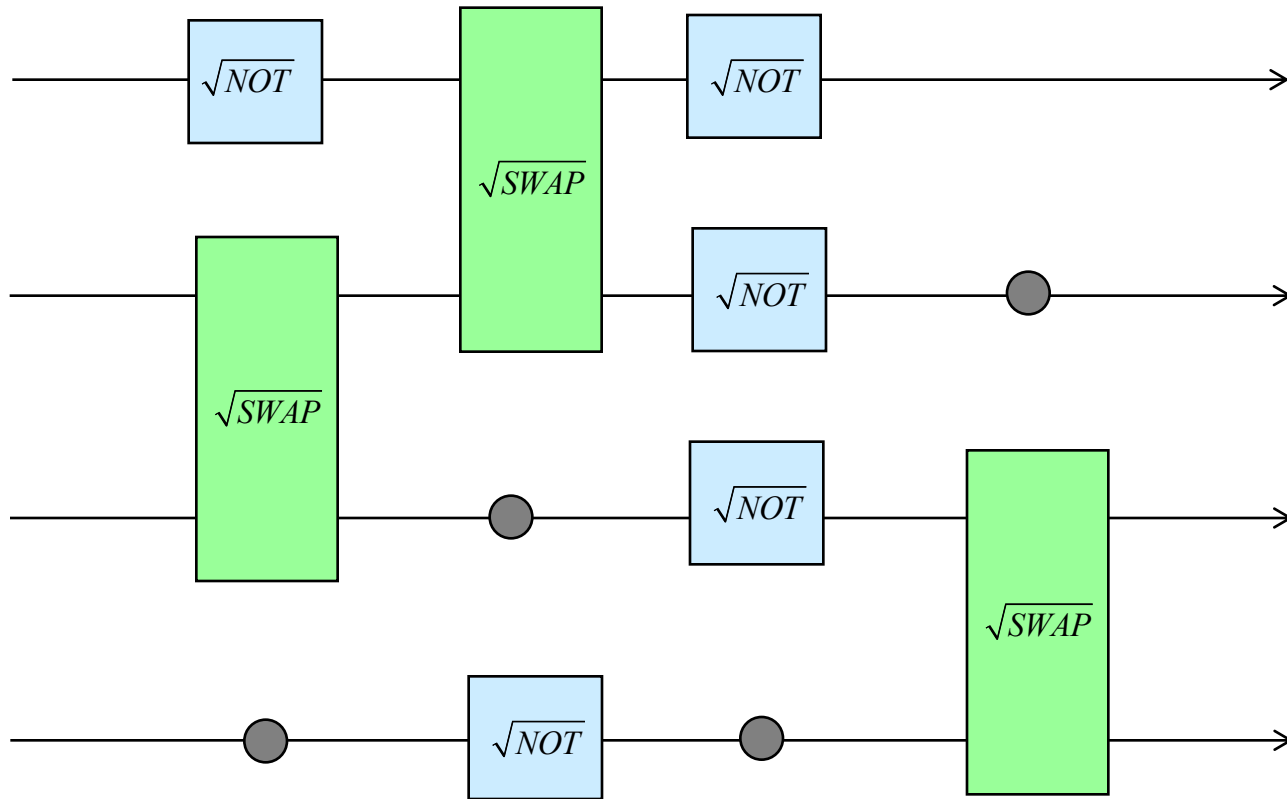
$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$$

**Innocuous phase gate
which makes all the difference**

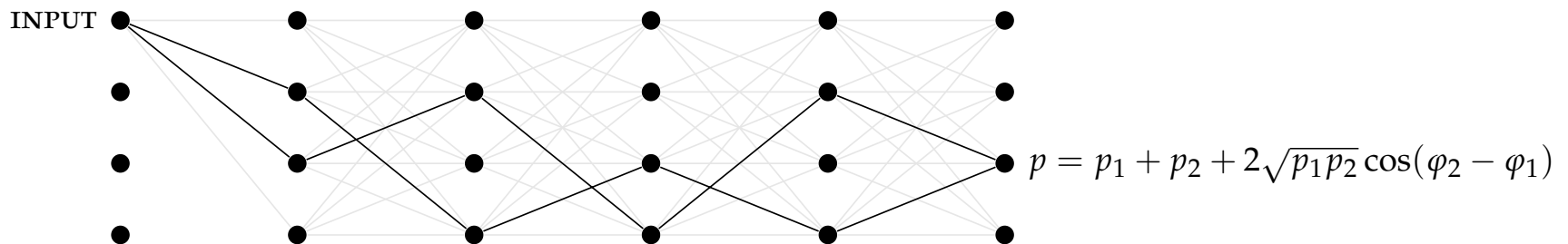
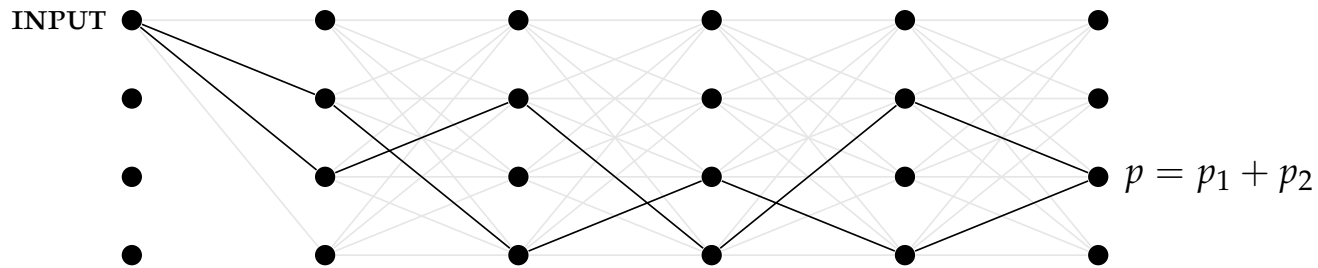
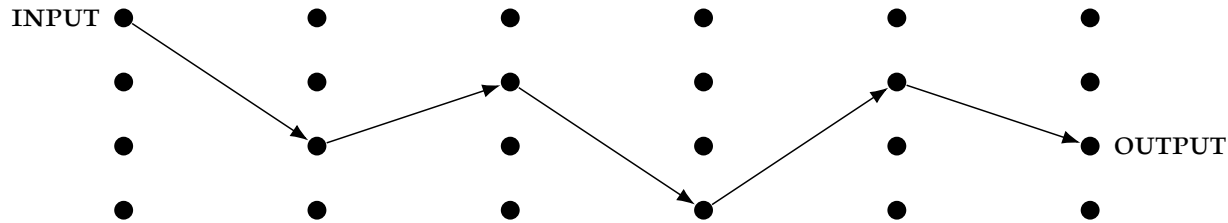
$$|0\rangle \rightarrow |0\rangle \quad |1\rangle \rightarrow e^{i\varphi} |1\rangle$$

Quantum circuits

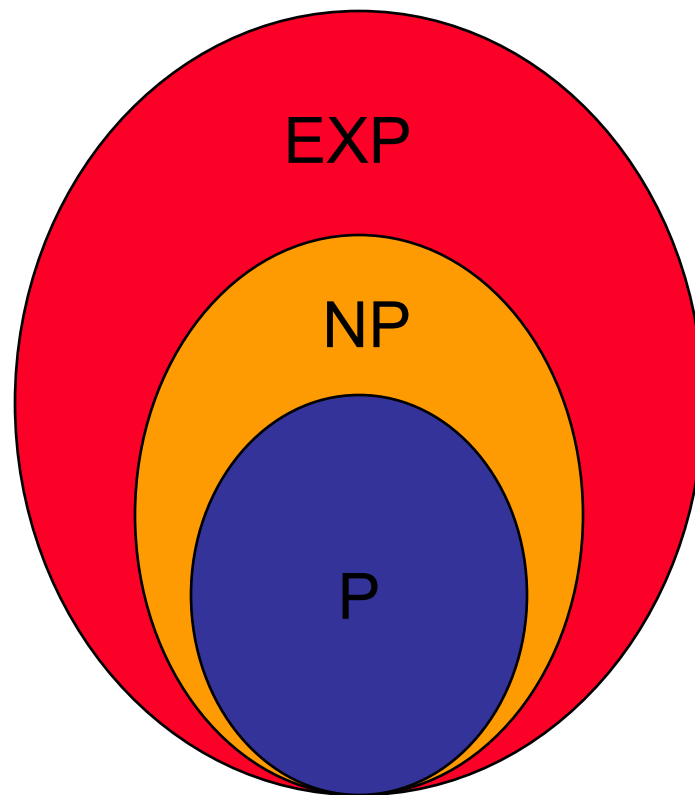
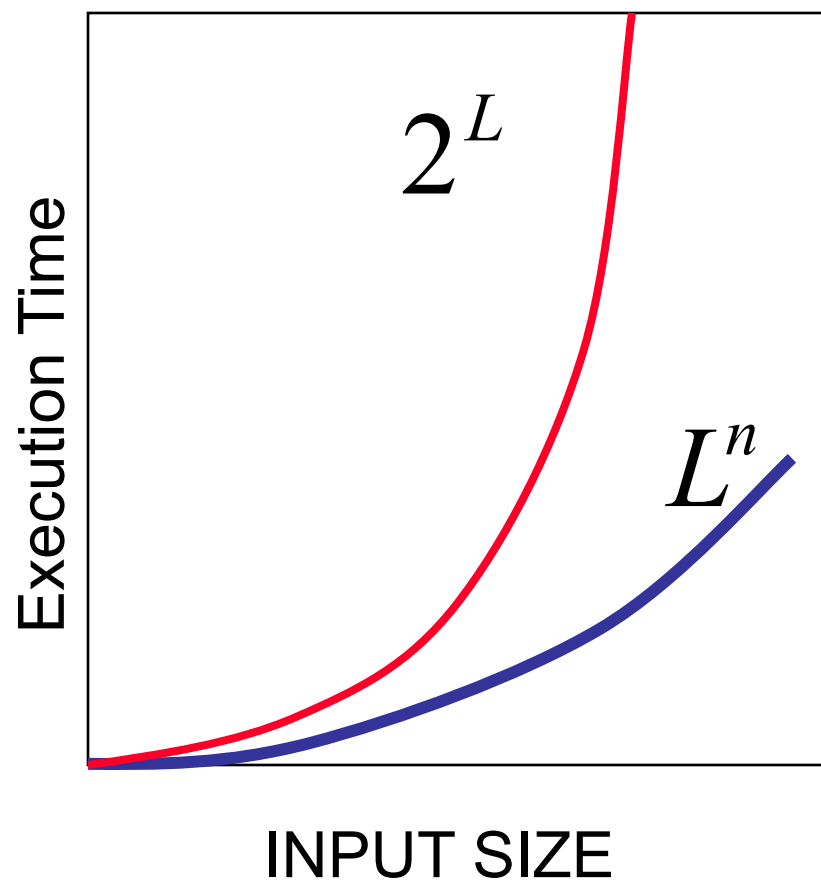
QUANTUM BITS = QUBITS



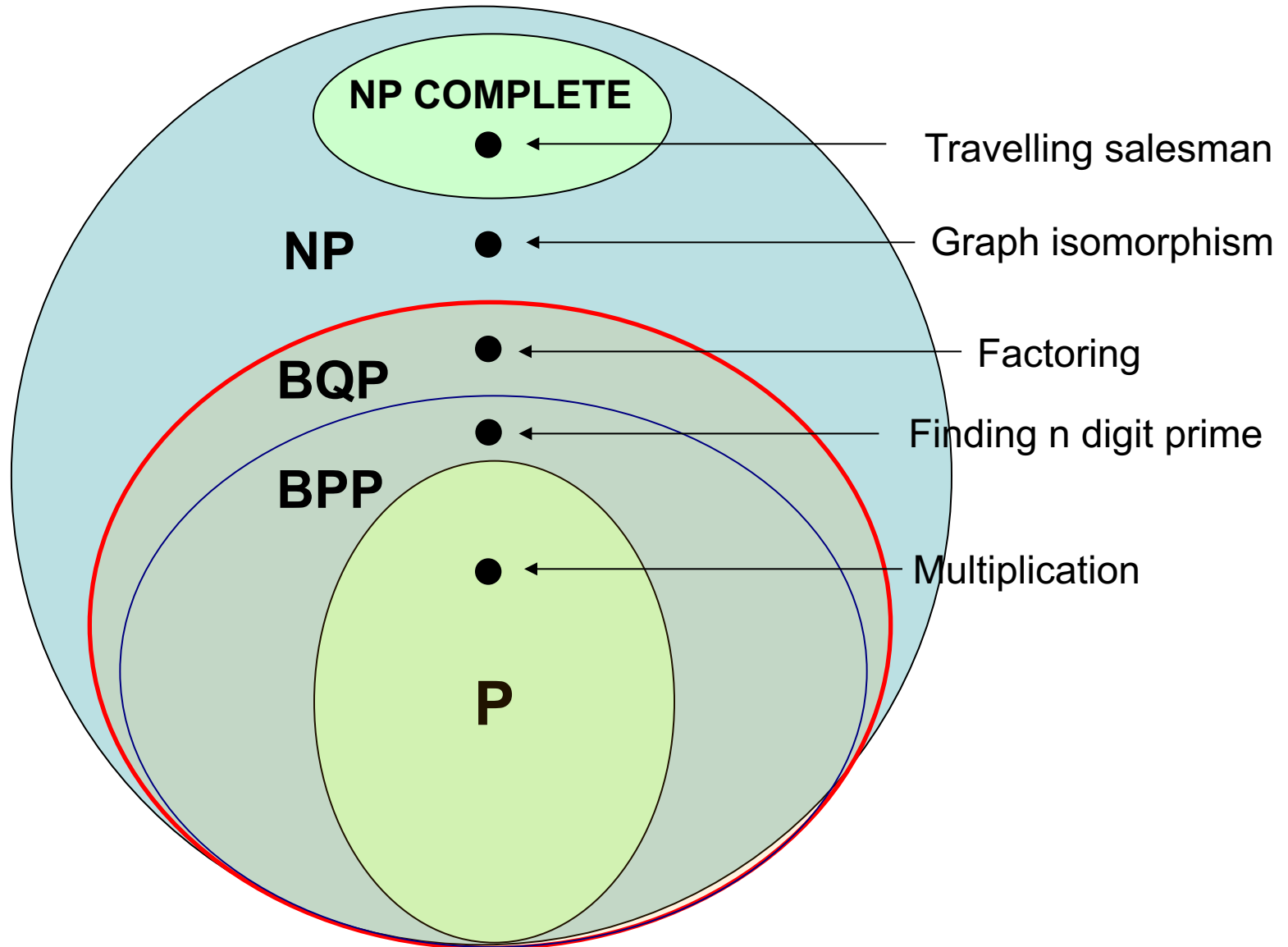
Deterministic, probabilistic and quantum



Hard and easy...



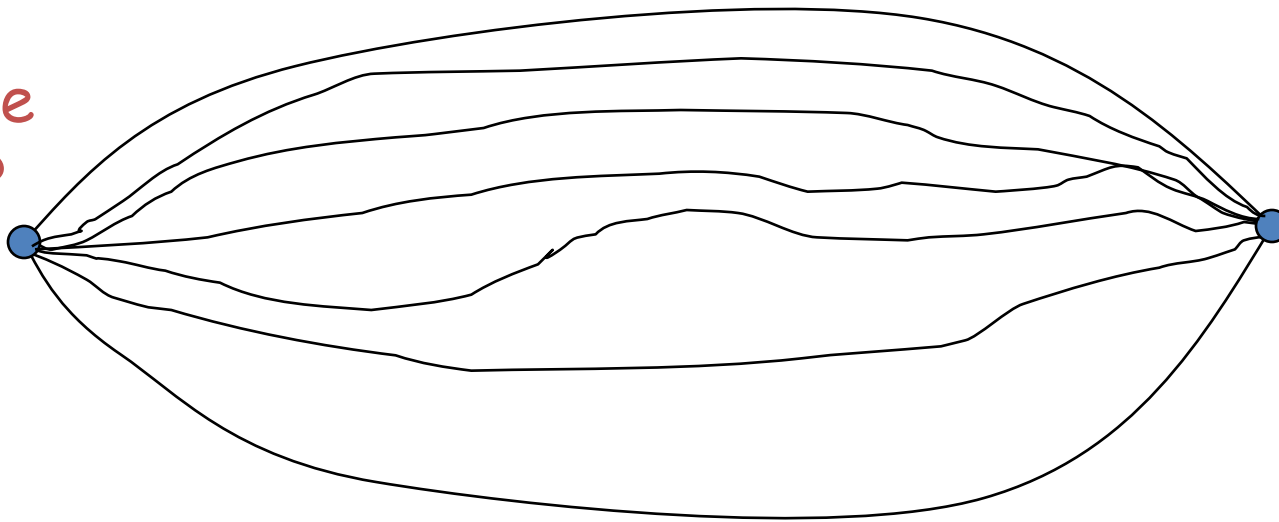
Zoo of computational complexity



Impact on logic...

Traditional approach: proof = physical record

Is **A** true
or not ?

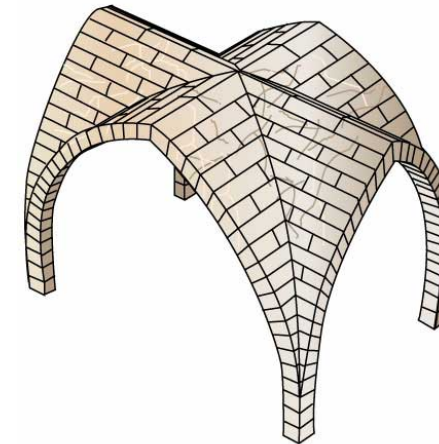
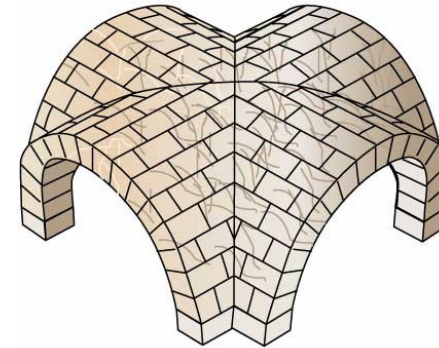
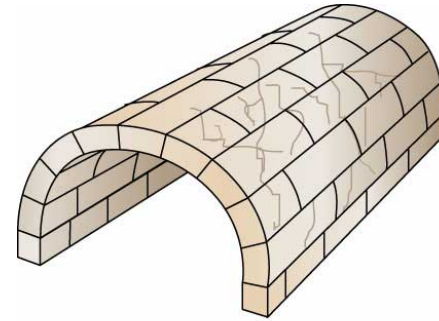


Yes, **A**
is true!

Testing 10^{100} different possibilities in quantum superpositions

Proof = physical process

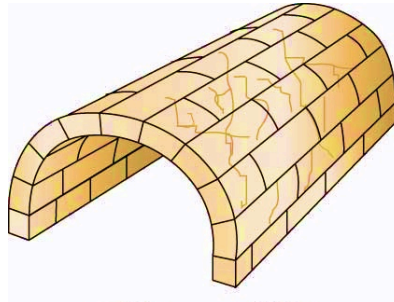
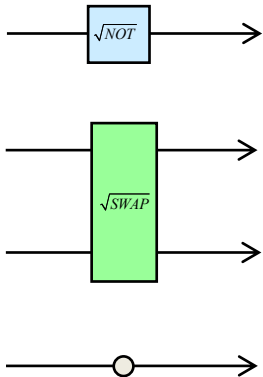
Limits to quantum computation ?



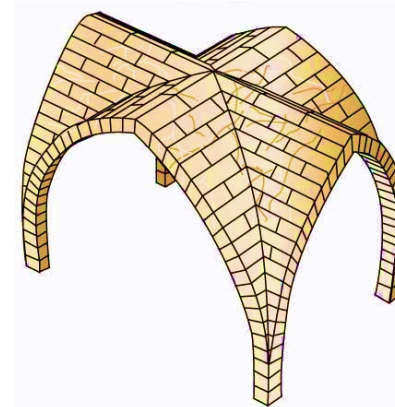
Building quantum computers...



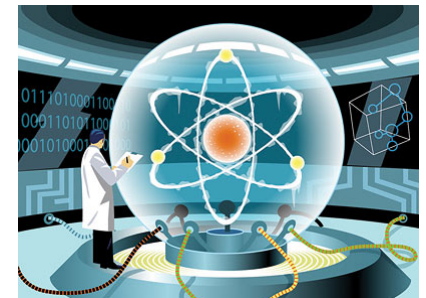
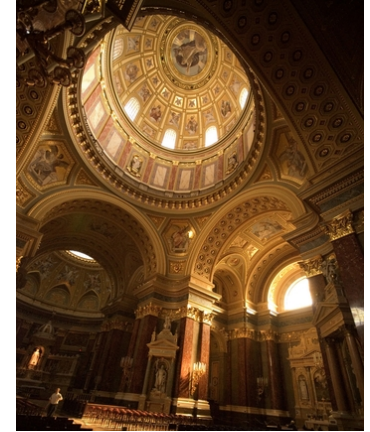
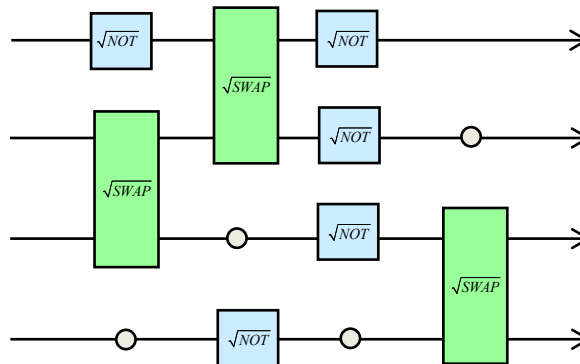
Basic blocks



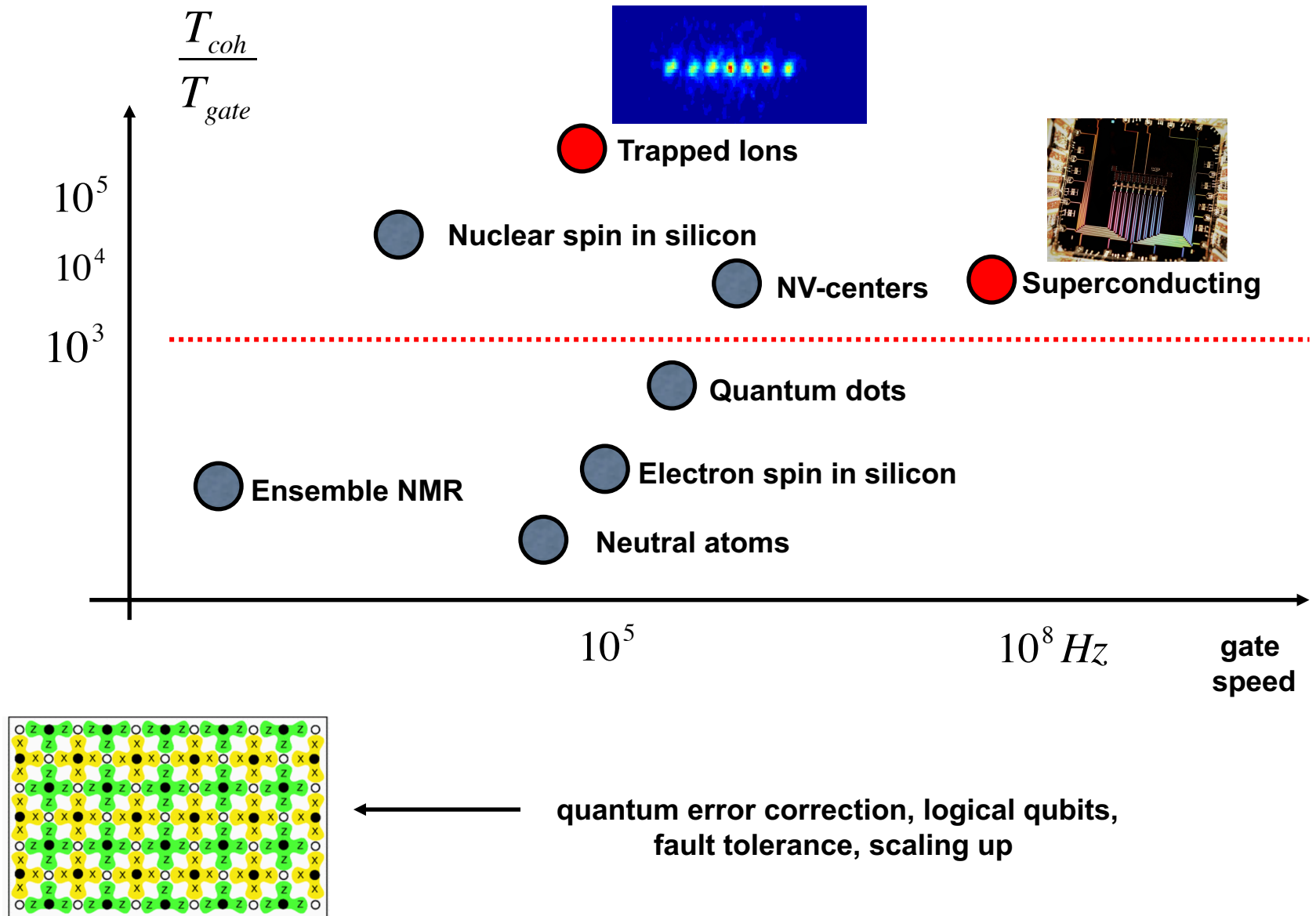
stable
fault tolerant



Scaling up



Practicalities...



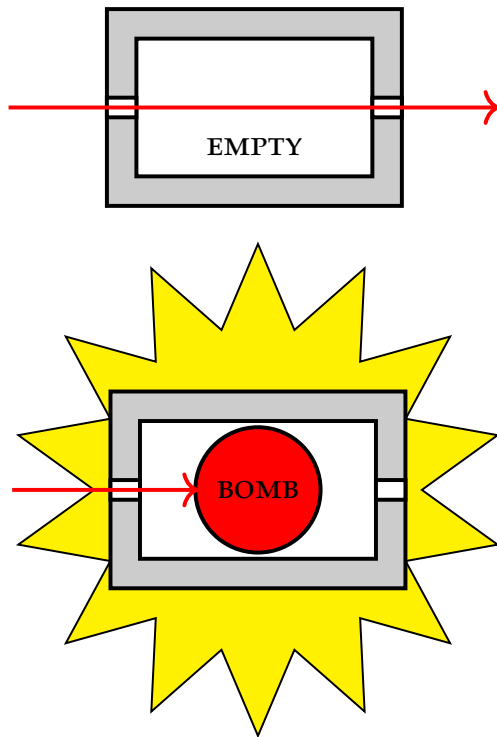
Do you understand complex numbers?

Here is a simple proof that $+1 = -1$,

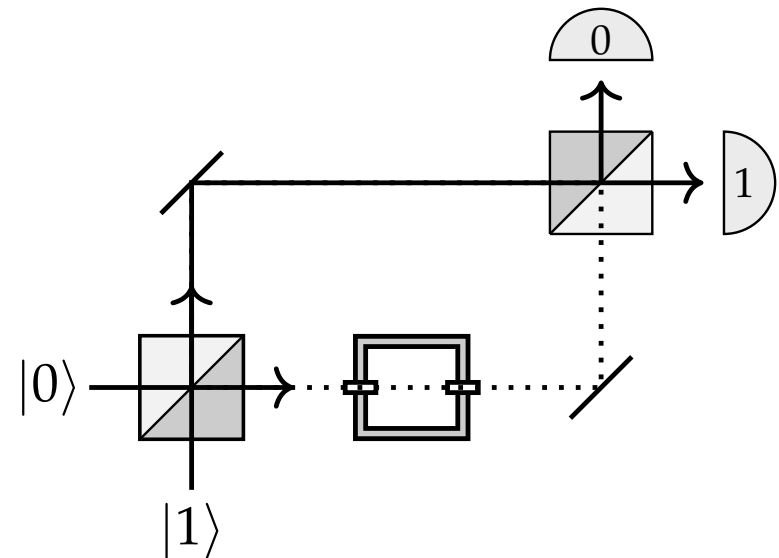
$$1 = \sqrt{1} = \sqrt{(-1)(-1)} = \sqrt{-1}\sqrt{-1} = i^2 = -1$$

What is wrong with it?

Can you detect super-sensitive bombs?



Hint: Consider the setup where the input and output ports are hooked up in one of the arms of a Mach-Zehnder interferometer.



Randomness...

...for the paranoid ones



Artur Ekert

Randomness – objective or subjective?

EPICURUS
(300 BC)

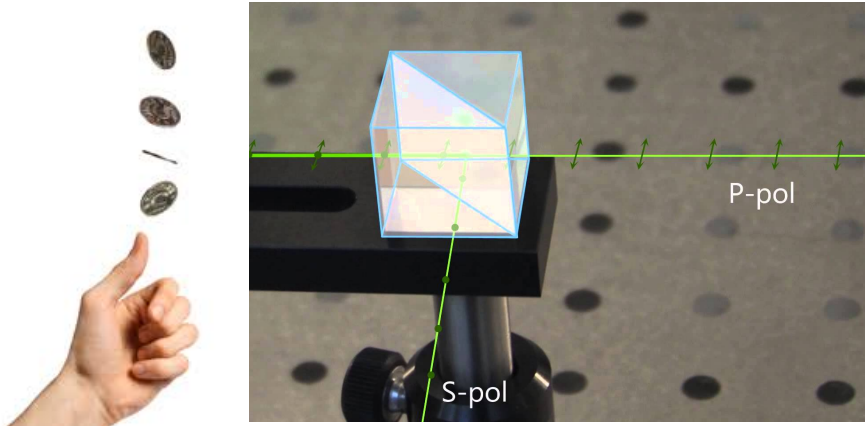
DEMOCRITUS
(400 BC)

atoms *swerve* at
random along
their paths

atoms follow
predetermined paths

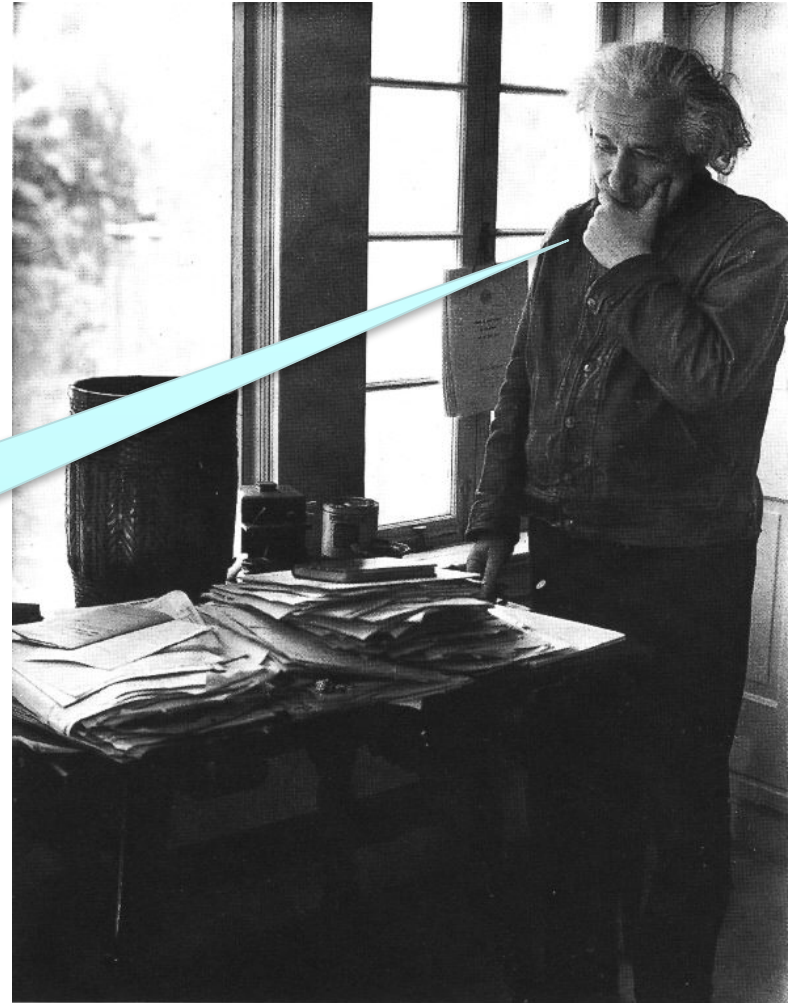
SUBJECTIVE

Objective, no way!



TRULY RANDOM?

...I would rather be a cobbler, or even an employee in a gaming-house, than a physicist.



The story of worry...

MAY 15, 1935

PHYSICAL REVIEW

VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in

quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.

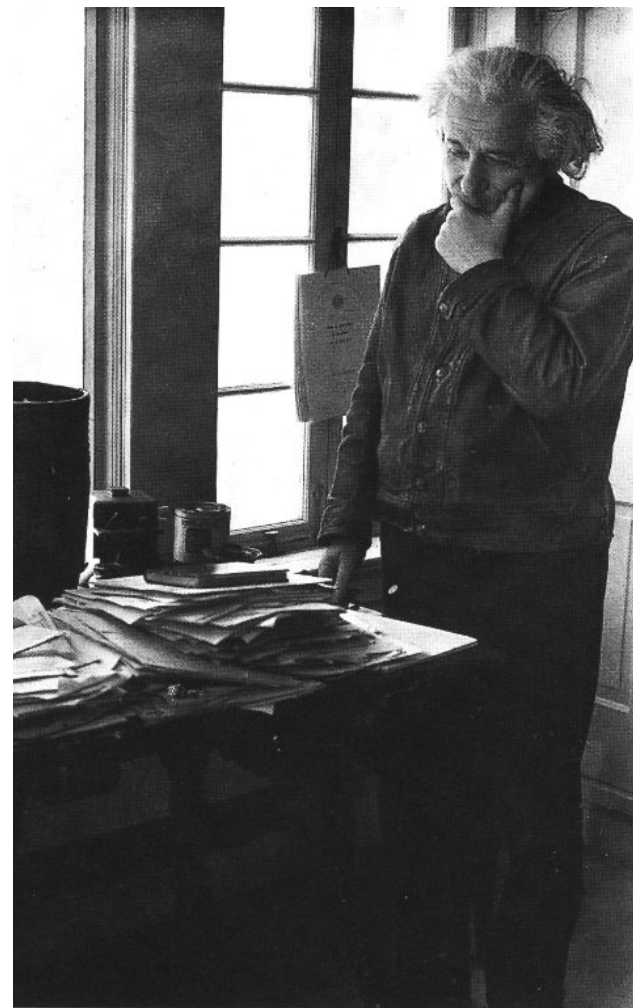
1.

ANY serious consideration of a physical theory must take into account the distinction between the objective reality, which is independent of any theory, and the physical concepts with which the theory operates. These concepts are intended to correspond with the objective reality, and by means of these concepts we picture this reality to ourselves.

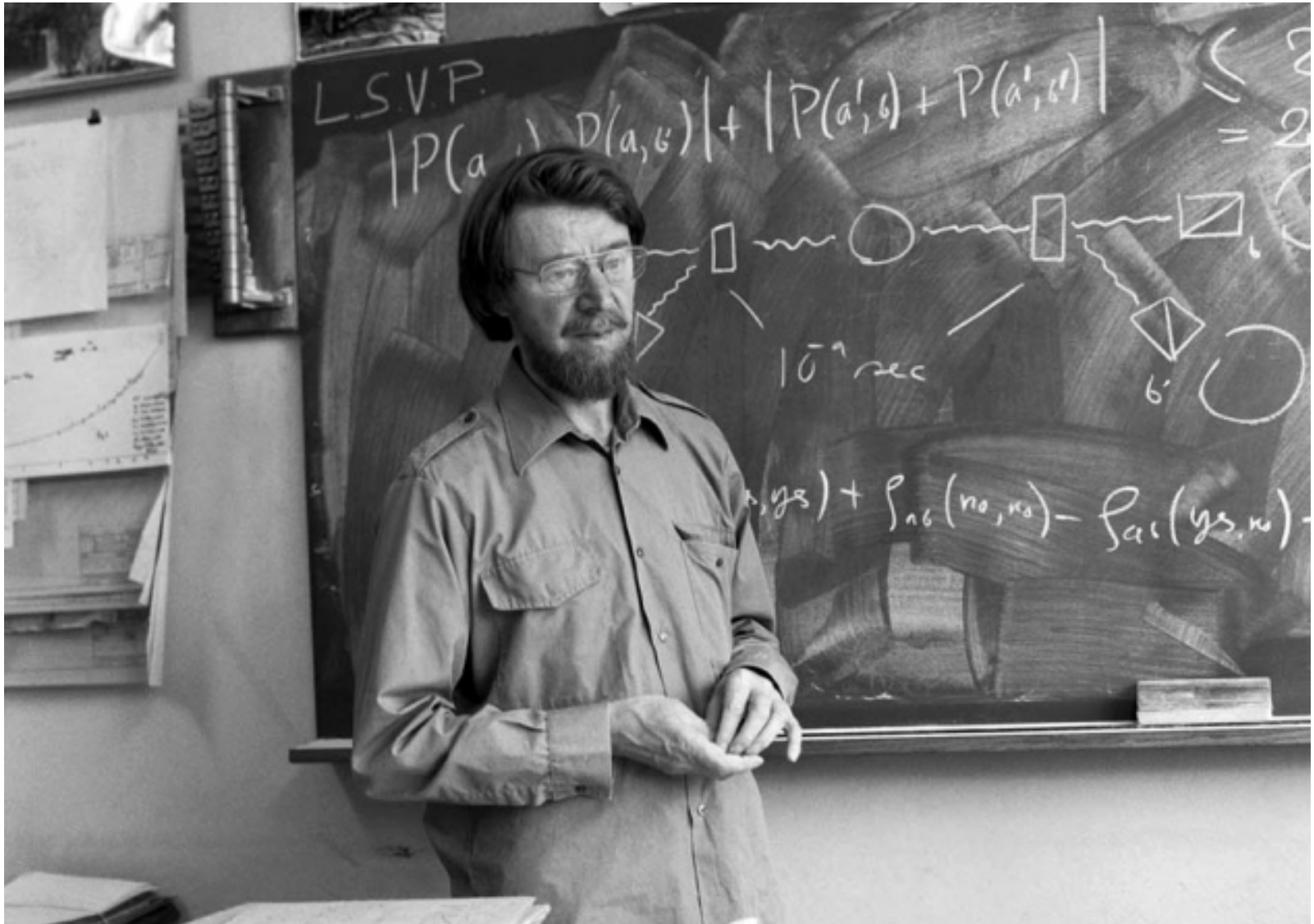
In attempting to judge the success of a physical theory, we may ask ourselves two questions: (1) "Is the theory correct?" and (2) "Is the description given by the theory complete?" It is only in the case in which positive answers may be given to both of these questions, that the concepts of the theory may be said to be satisfactory. The correctness of the theory is judged by the degree of agreement between the conclusions of the theory and human experience. This experience, which alone enables us to make inferences about reality, in physics takes the form of experiment and measurement. It is the second question that we wish to consider here, as applied to quantum mechanics.

Whatever the meaning assigned to the term *complete*, the following requirement for a complete theory seems to be a necessary one: *every element of the physical reality must have a counterpart in the physical theory*. We shall call this the condition of completeness. The second question is thus easily answered, as soon as we are able to decide what are the elements of the physical reality.

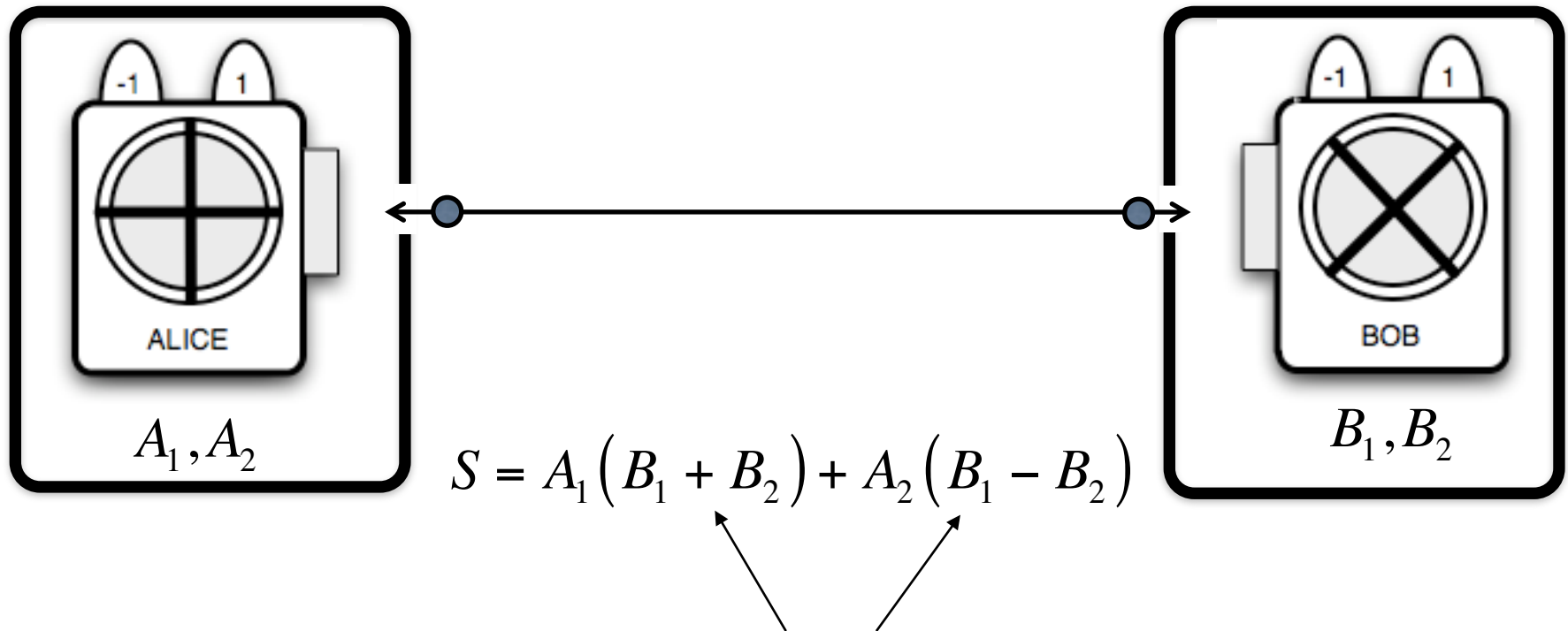
The elements of the physical reality cannot be determined by *a priori* philosophical considerations, but must be found by an appeal to results of experiments and measurements. A comprehensive definition of reality is, however, unnecessary for our purpose. We shall be satisfied with the following criterion, which we regard as reasonable. *If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity*. It seems to us that this criterion, while far from exhausting all possible ways of recognizing a physical reality, at least provides us with one



John Bell: it is a testable proposition...



Bell's inequalities...



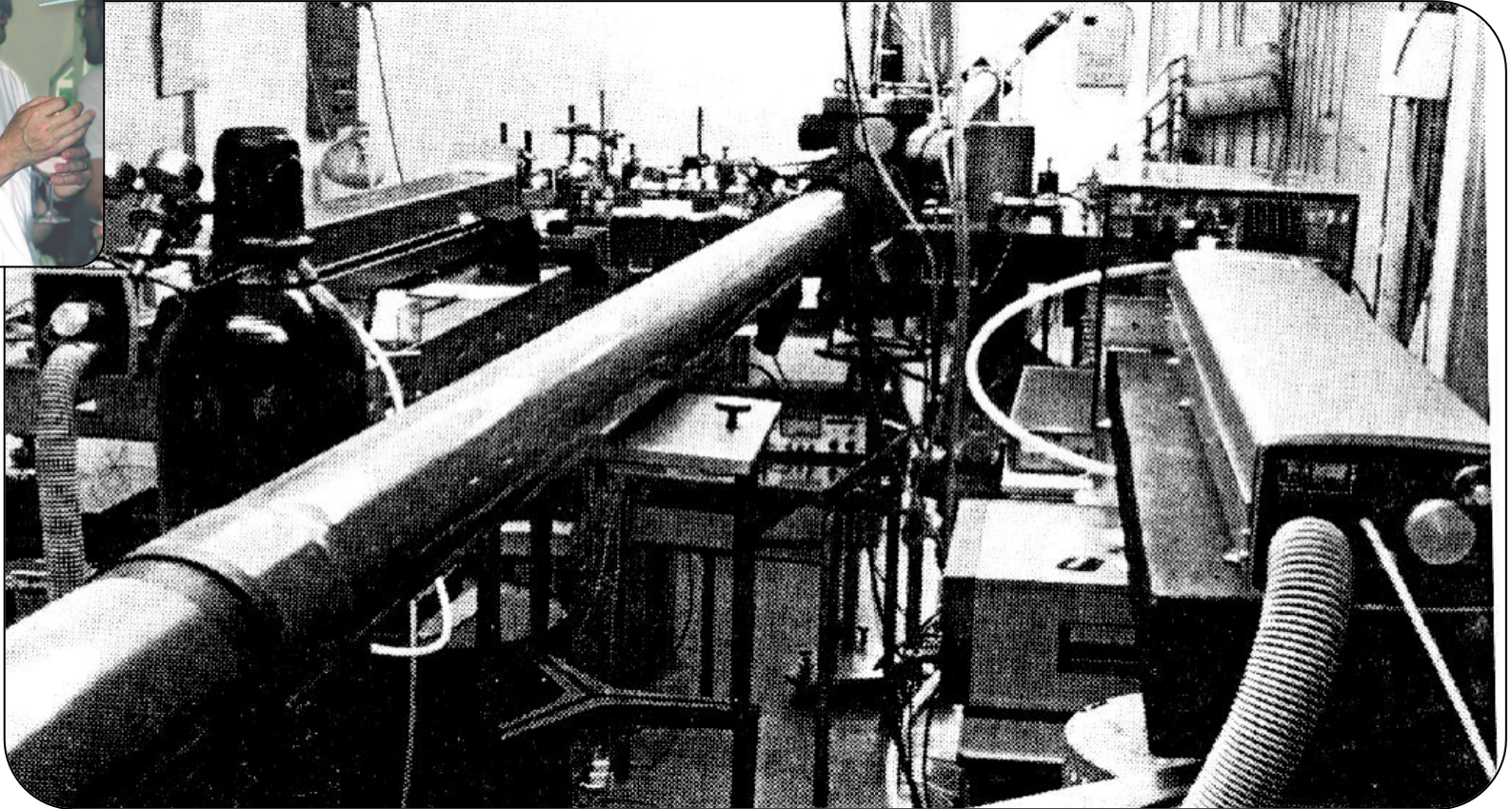
One of these terms is 0 and the other is ± 2

$$S = \pm 2 \quad \text{hence} \quad -2 \leq \langle S \rangle \leq 2$$

Almost twenty years later...

Alain Aspect

OBJECTIVE!
And it can be demonstrated!



Institut d'Optique d'Orsay (1982)

Uniformly distributed and unpredictable



0100010110011111001010100010...

EACH BIT MUST BE



UNIFORMLY DISTRIBUTED



INDEPENDENT OF ANYTHING ELSE (OUTSIDE ITS FUTURE LIGHT CONE)



**CERTIFICATION OF
THE PROCESS**

Trust the authorities?

CTL
COMPLIANCE TESTING LABORATORY

Certificate of Compliance

This is to certify that the Random Number Generator

Quantis-v10.10.08

by

ID Quantique SA

REF : CTL-037/37001

has been tested by

CTL, Compliance Testing Laboratory

and has been found to be *suitably unpredictable and fit for purpose*

Issue Date: 30.03.2011

Quantis USB
Serial n° 090615A410

Technical Compliance Manager, CAST Limited

UKAS
TESTING

CAST

BANGOR
UNIVERSITY

CAST LTD Compliance Testing Laboratory,
A company approved and certified under the Online Gambling Regulation Act 2001 and accredited by UKAS for UK Testing

Compliance Testing Laboratory, Tŷ Menai, Fford Penlan, Parc Menai Business Park, Bangor, Gwynedd
LL57 4HJ

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Justice and Police FDJP
Federal Office of Metrology METAS

Certificate of Conformity No 151-04687

Object	Quantum Random Number Generator Quantis-USB S/N 070222A410 Quantis-PCI-1 S/N 08338A310 Quantis-PCI Express S/N 1002251A210
Applicant	id Quantique SA Ch. De la Marbrerie 3 1227 Carouge/Geneva Switzerland
Requirements	The output of the Quantis random number generator has to pass all DIEHARD Battery of Tests, confirming that the random number generator distributes numbers with sufficient non-predictability, fair distribution and lack of bias to particular outcomes. Specifically: 10 data sets consisting of 1E8 bits per data set is considered to be random if none of the 234 p-values produced by the 15 DIEHARD Battery of Tests has a value between 1 and 1-epsilon, where epsilon is 1e-6.
Confirmation	The tested Quantis-USB, Quantis-PCI-1 and Quantis-PCI Express have passed all DIEHARD Battery of Tests. The sequence of random bits generated cannot be predicted. The sequence of random bits generated cannot be reproduced.
Remarks	The testing procedure used is described in the annex document "Annex_METAS_151-04687"

CH-3003 Bern-Wabern, 10 May 2010

For the Test

Dr.Damian Twerenbold

Division Mechanics, Radiation and Time

Dr.Philippe Richard, Vice-Director

This document may not be published or forwarded other than in full.

METAS
Lindemweg 50, CH-3003 Bern-Wabern, Tel. +41 31 33 33 111, www.metas.ch

1/1

Device independent verification



0100010110011111001010100010...

EACH BIT MUST BE

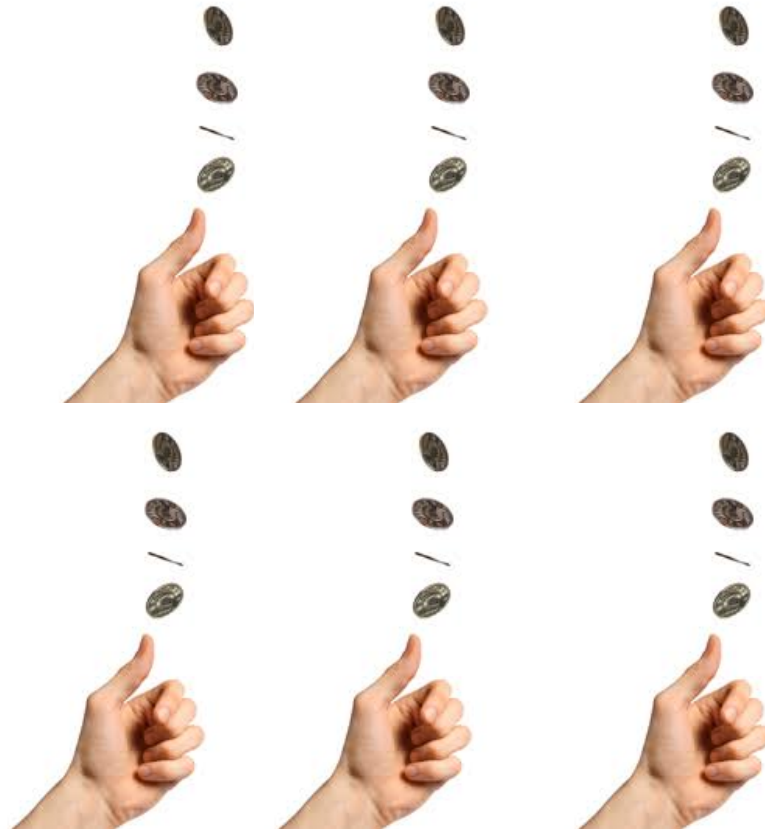
- ✓ **UNIFORMLY DISTRIBUTED**
- ✓ **INDEPENDENT OF ANYTHING ELSE (OUTSIDE ITS FUTURE LIGHT CONE)**



**No need for
certification!
No need to trust
authorities!
Tested by users**

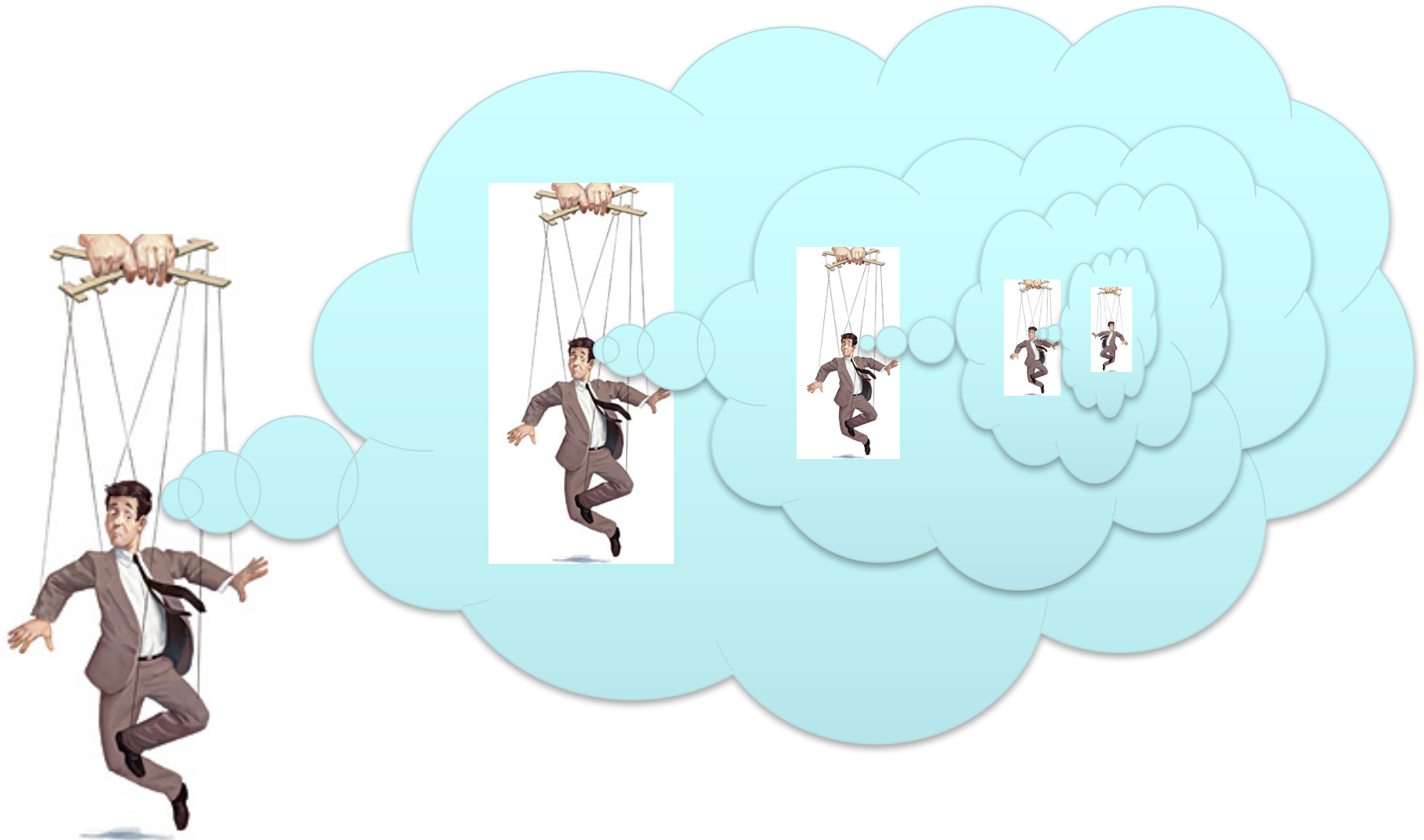
Verification requires some randomness...

...or free will!



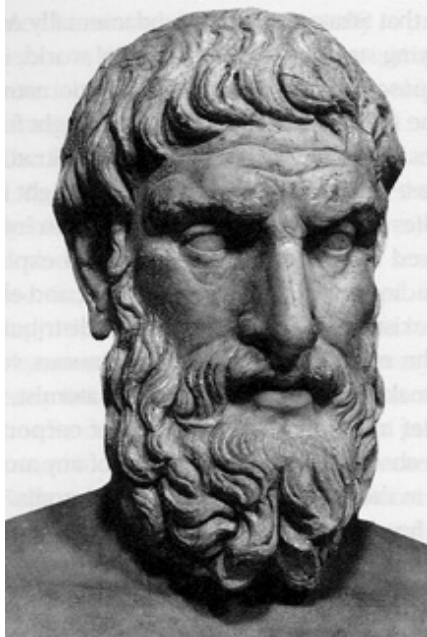
Randomness amplification

Free will within deterministic system



nothing to do with randomness

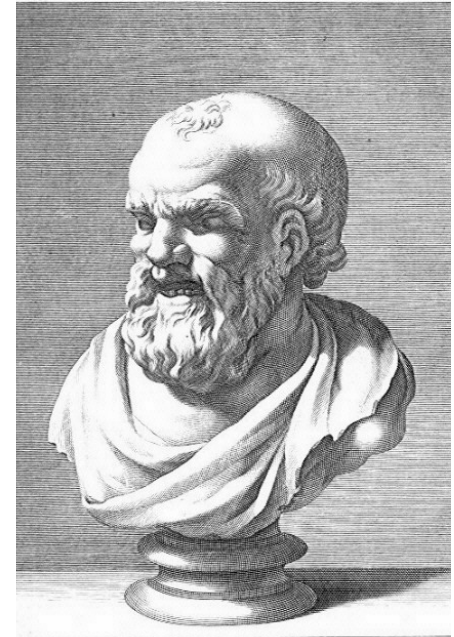
Beyond the simplistic mathematical model



EPICURUS
(300 BC)

OBJECTIVE

If everything is quantum
then
what is randomness?



DEMOCRITUS
(400 BC)

SUBJECTIVE

Many open questions



EPR VISION OF REALITY IS TOO SIMPLISTIC



SECURITY AND RANDOMNESS IN THE MULTIVERSE