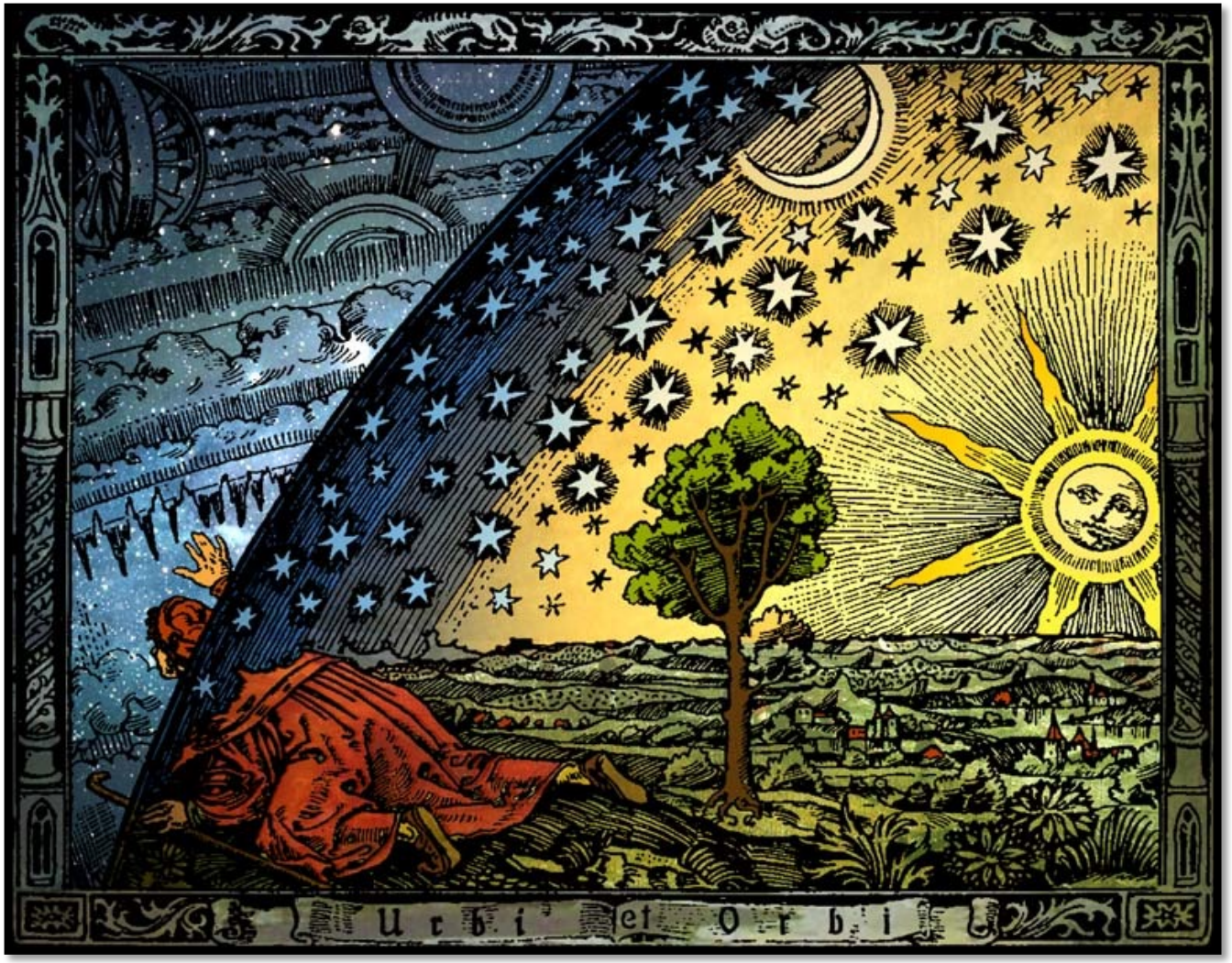


QUANTUM CONNECTIONS

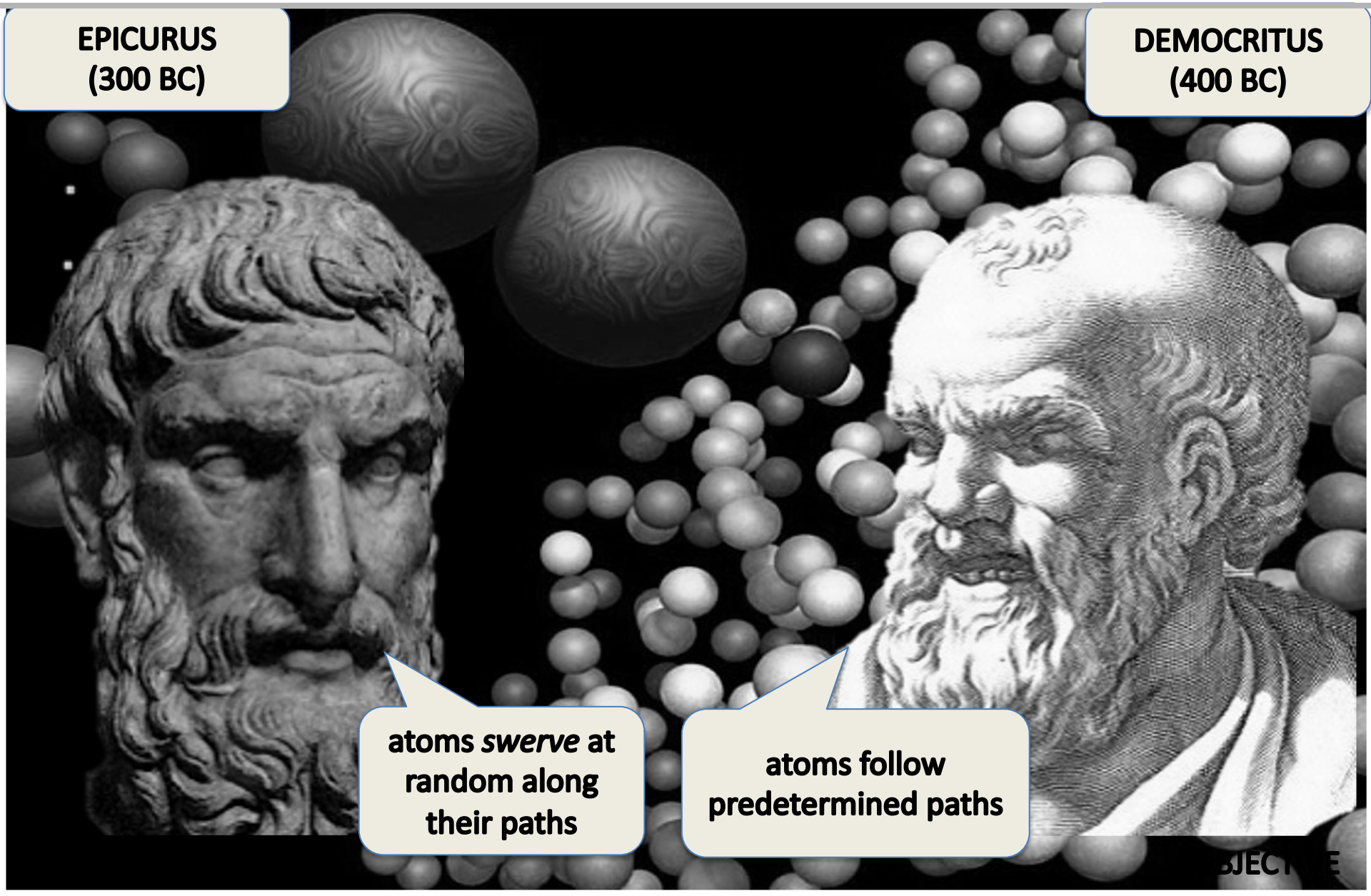
Artur Ekert

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, Alibaba or John Doe build a quantum computer?

Artur Ekert
Mathematical Institute, University of Oxford
CQT, National University of Singapore
OIST, Japan

Randomness – objective or subjective?



Determinism, free will & moral responsibility

The Last Judgement, Hieronymus Bosch (1482)

More pragmatic approach - gambling

Caravaggio, The Cardsharps c. 1594

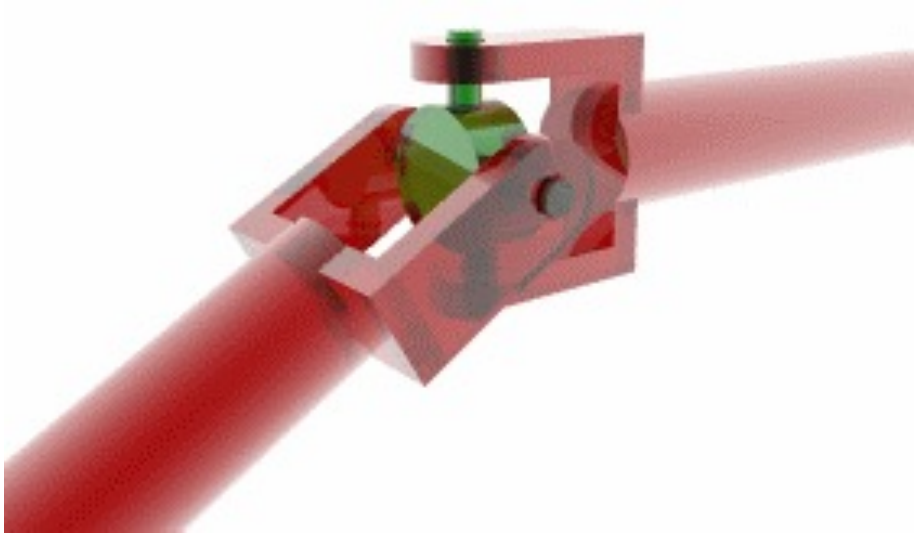
Girolamo Cardano - Gambling Scholar

1501-1576

Cardano described himself as

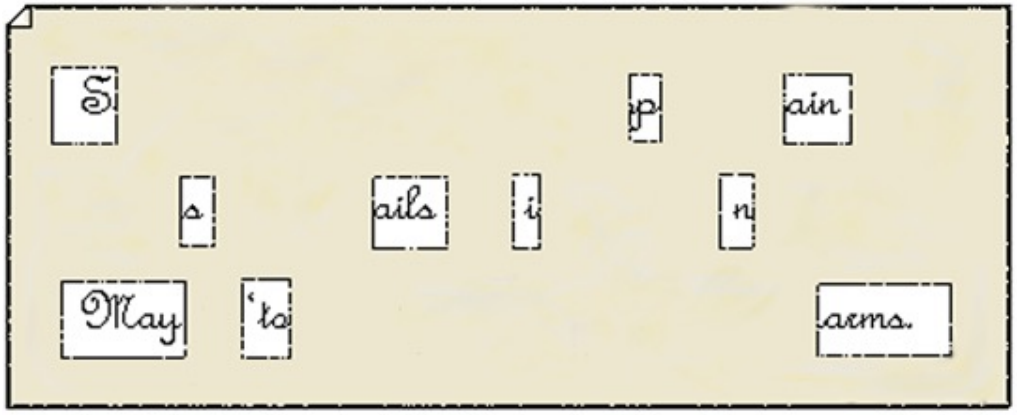
Hot-tempered, single-minded, and given to women, …cunning, crafty, sarcastic, diligent, impertinent, sad, treacherous, magician and sorcerer, miserable, hateful, lascivious, obscene, lying, obsequious,…fond of the prattle of old men.

Cardano’s shaft joint

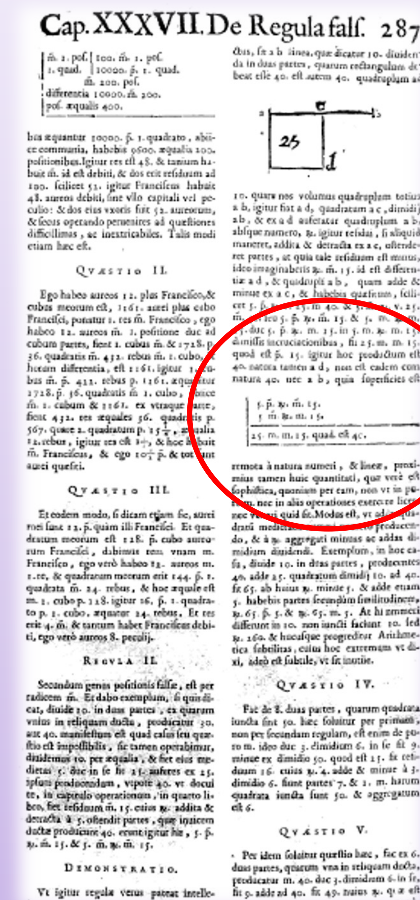


Cardano's grille

Sir John regards you well and spekes again that
all as rightly 'vails him is yours now and ever.
May he 'tone for past d'lays with many charms.



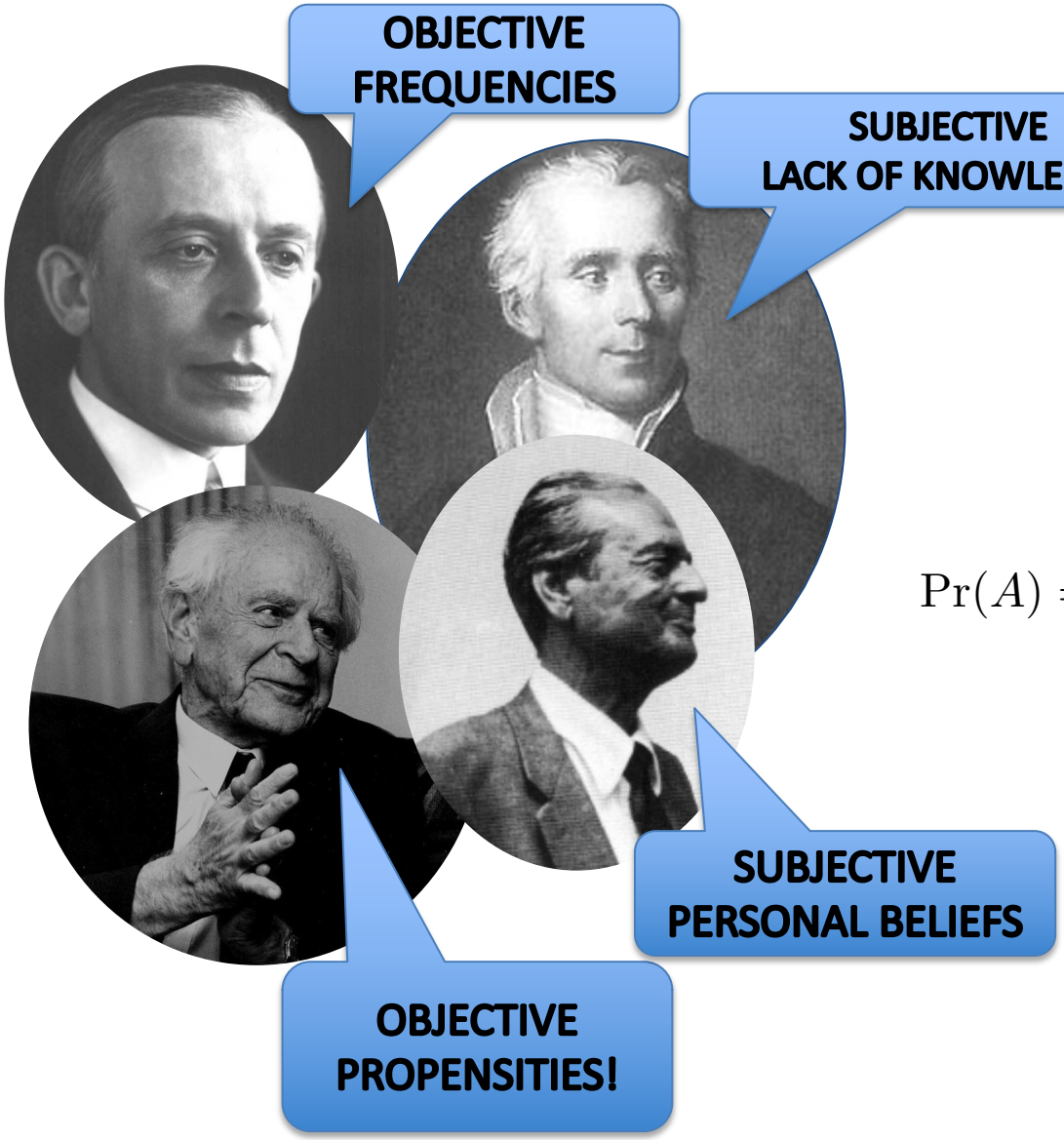
Probability and complex numbers



PROBABILITY
Liber de Ludo Aleae

COMPLEX NUMBERS
Ars Magna

What is probability…



To measure probability find
equally probable
cases and count them

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

And then came Kolmogorov…

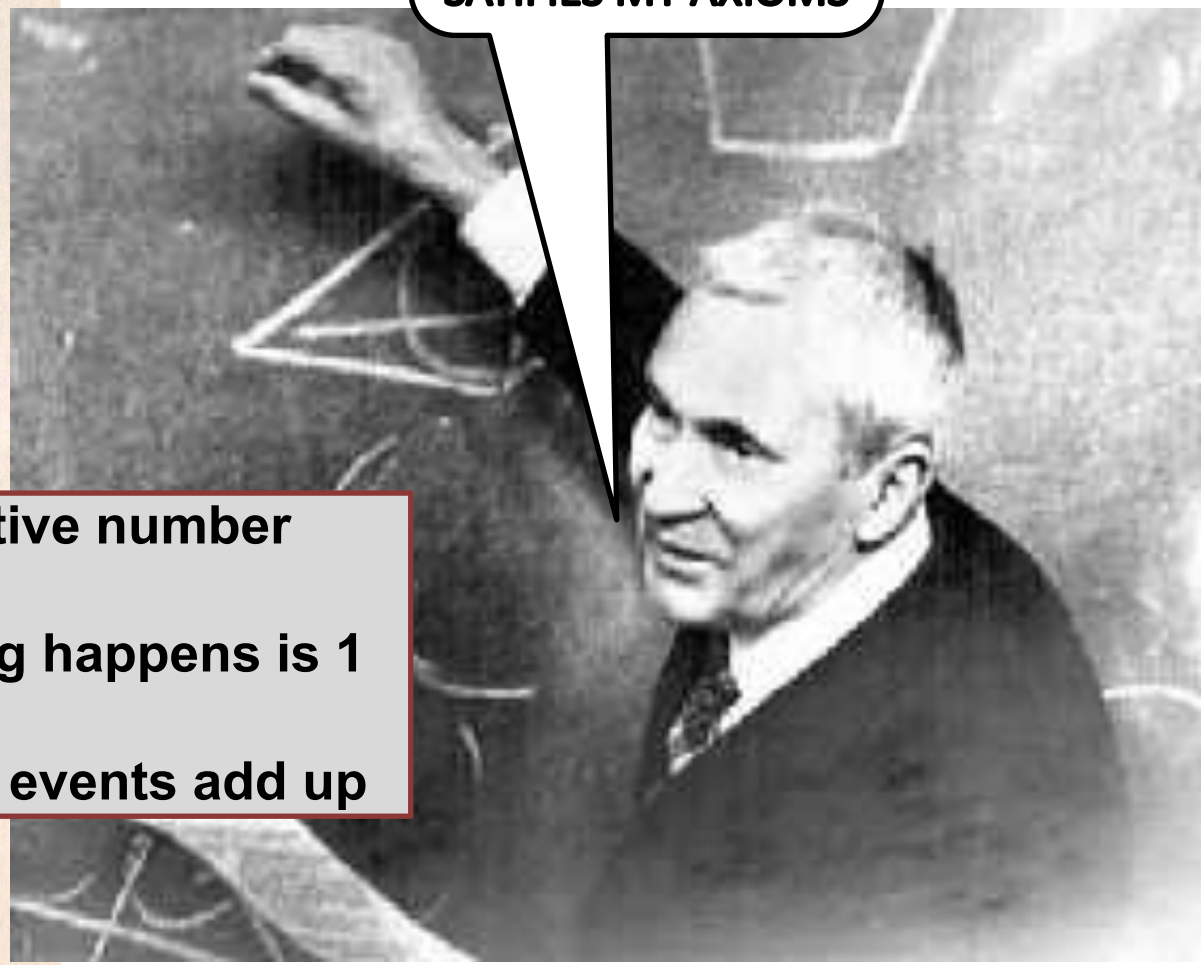
ERGEBNISSE DER MATHEMATIK
UND IHRER GRENZGEBIETE
HERAUSGEGEBEN VON DER SCHRIFTLEITUNG
DES
„ZENTRALBLATT FÜR MATHEMATIK"
ZWEITER BAND
3

GRUNDBEGRIFFE DER
WAHRSCHEINLICHKEITS-
RECHNUNG

VON

A. KOLMOGOROFF

BERLIN
VERLAG VON JULIUS SPRINGER
1933



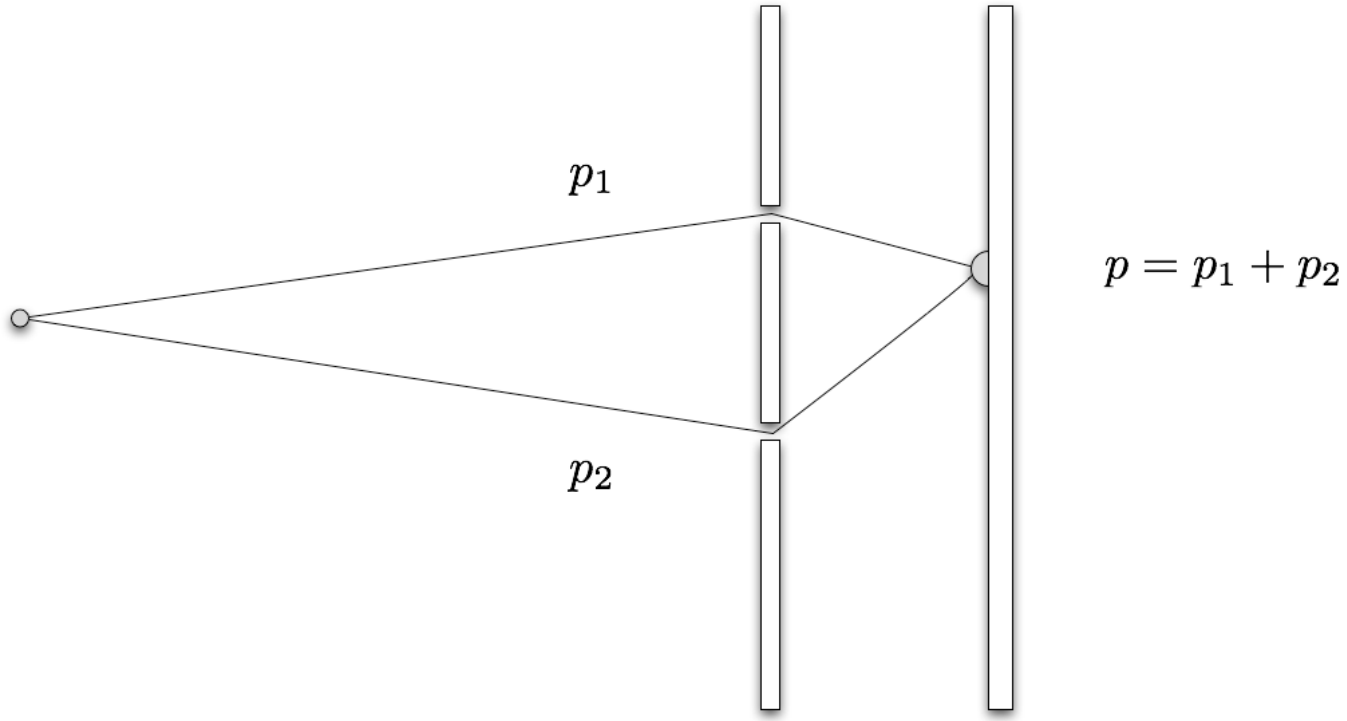
Probability is a non-negative number

Probability that something happens is 1

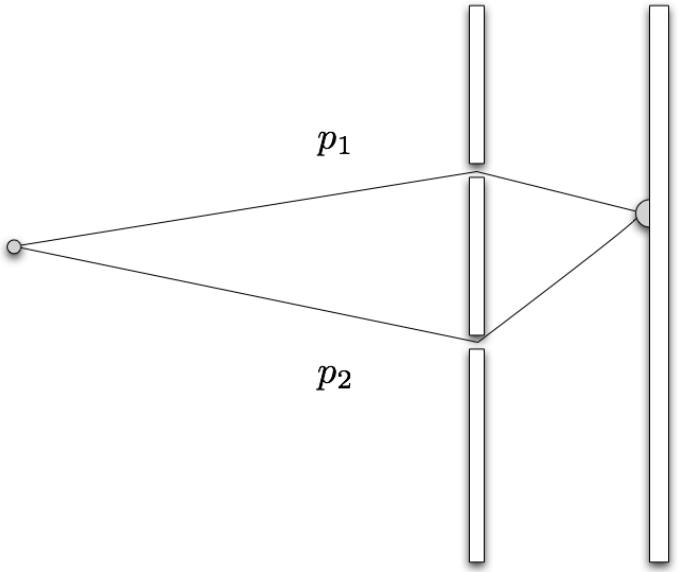
Probabilities of exclusive events add up

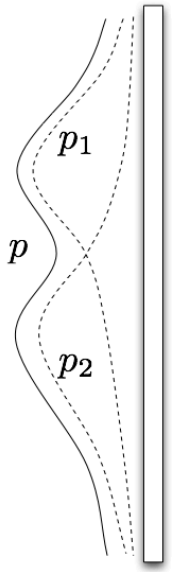
Additivity axiom

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.

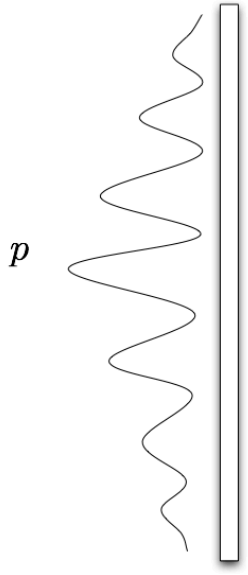


Nature ignores additivity axiom

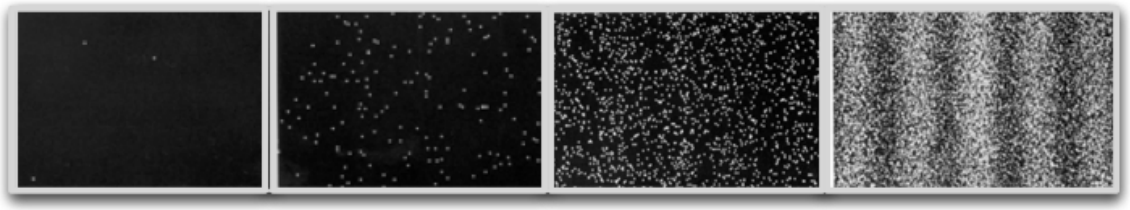




THIS IS WHAT YOU EXPECT

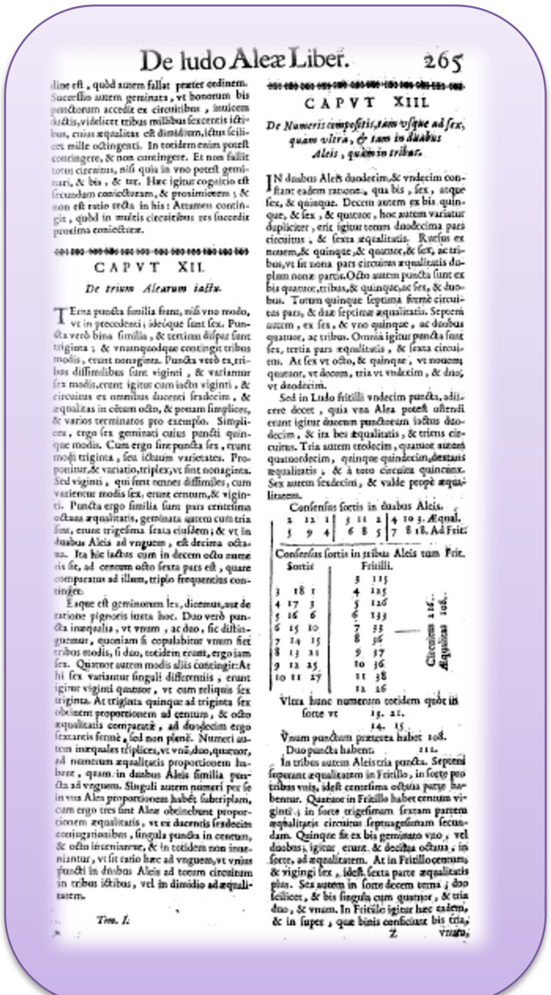


THIS IS WHAT YOU OBSERVE



HITACHI DOUBLE SLIT EXPERIMENT WITH INDIVIDUAL ELECTRONS

Back to Cardano

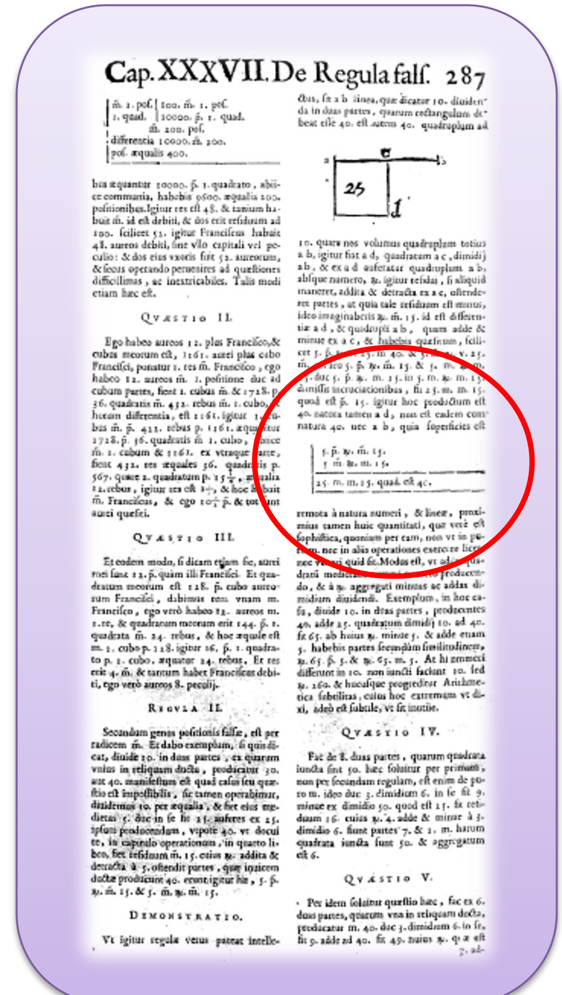

De ludo Aleæ Liber. 265

CAPVT XII

De trium Alearum iactu.

CAPVT XIII

1501-1576


Cap. XXXVII. De Regula falſ. 287

PROBABILITY
Liber de Ludo Aleae

COMPLEX NUMBERS
Ars Magna

Enter complex numbers

10. quare nos volumus quadruplum totius a b, igitur fiat a d, quadratum a c, dimidij a b, & ex a d auferatur quadruplum a b, absque numero, ℞. igitur residui, si aliquid maneret, addita & detracta ex a c, ostenderet partes, at quia tale residuum est minus, ideo imaginaberis ℞. m̃. 15. id est differentiæ a d, & quadrupli a b, quam adde & minue ex a c, & habebis quæsitum, scilicet 5. p̃. ℞. v. 25. m̃. 40. & 5. m̃. ℞. v. 25. m̃. 40. seu 5. p̃. ℞. m̃. 15. & 5. m. ℞. m. 15. duc 5. p̃. ℞. m. 15. in 5. m. ℞. m. 15. dimissis incruciationibus, fit 25. m. m. 15. quod est p̃. 15. igitur hoc productum est 40. natura tamen a d, non est eadem cum natura 40. nec a b, quia superficies est

5. p̃. ℞. m̃. 15.
5 m̃. ℞. m. 15.
25. m. m. 15. quad. est 40.

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

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

$$25-(-15)$$

$$25+15$$

$$40$$

Complex numbers

$$\alpha = a + i\,b$$

$$i = \sqrt{-1} \qquad i^2 = -1$$

Modern notation

Karl Friedrich Gauss

1777-1855

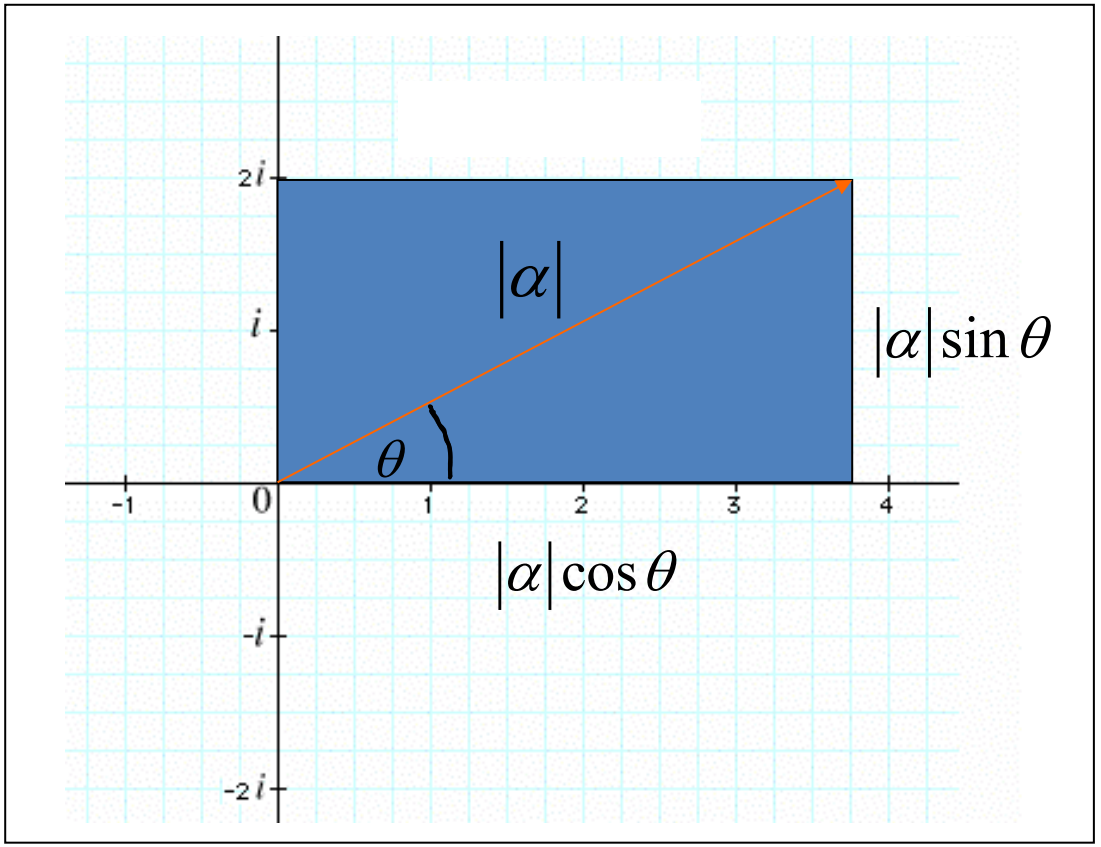
$3 + i\,42 \quad \sqrt{6} \quad \sqrt{-6} = i\sqrt{6}$

purely real **purely imaginary**

Geometric representation

Leonhard Euler
1707-1783

$$\alpha = a + ib = |\alpha|(\cos\theta + i\sin\theta) = |\alpha| e^{i\theta}$$



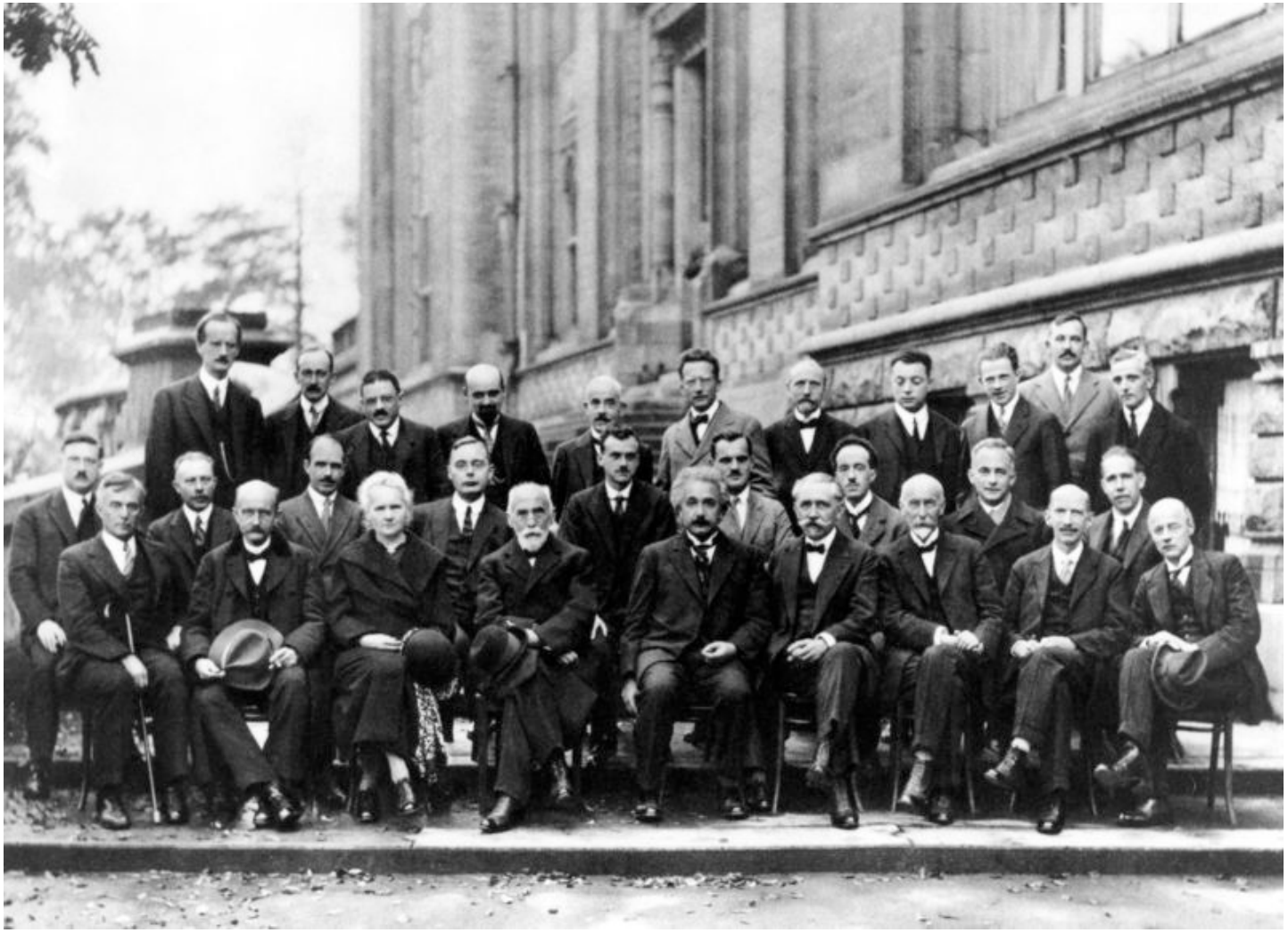
Do you understand complex numbers?

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?

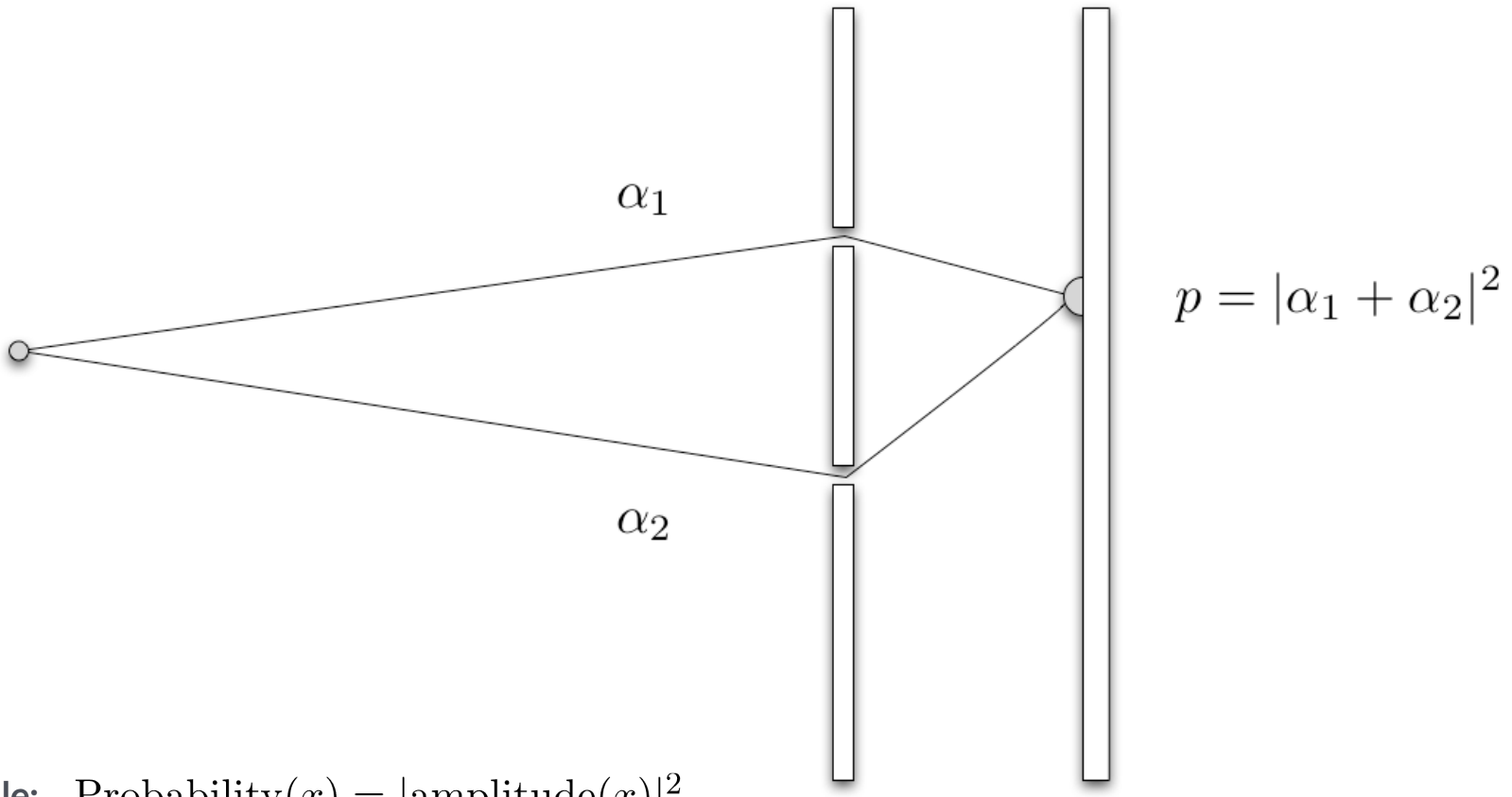
Enter quantum theory



The Solvay Congress 1927

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.



Born Rule: $\text{Probability}(x) = |\text{amplitude}(x)|^2.$

Born Rule: $\text{Probability}(x) = |\text{amplitude}(x)|^2.$

THE QUANTUM MECHANICS OF COLLISIONS

[Preliminary communication]†

MAX BORN

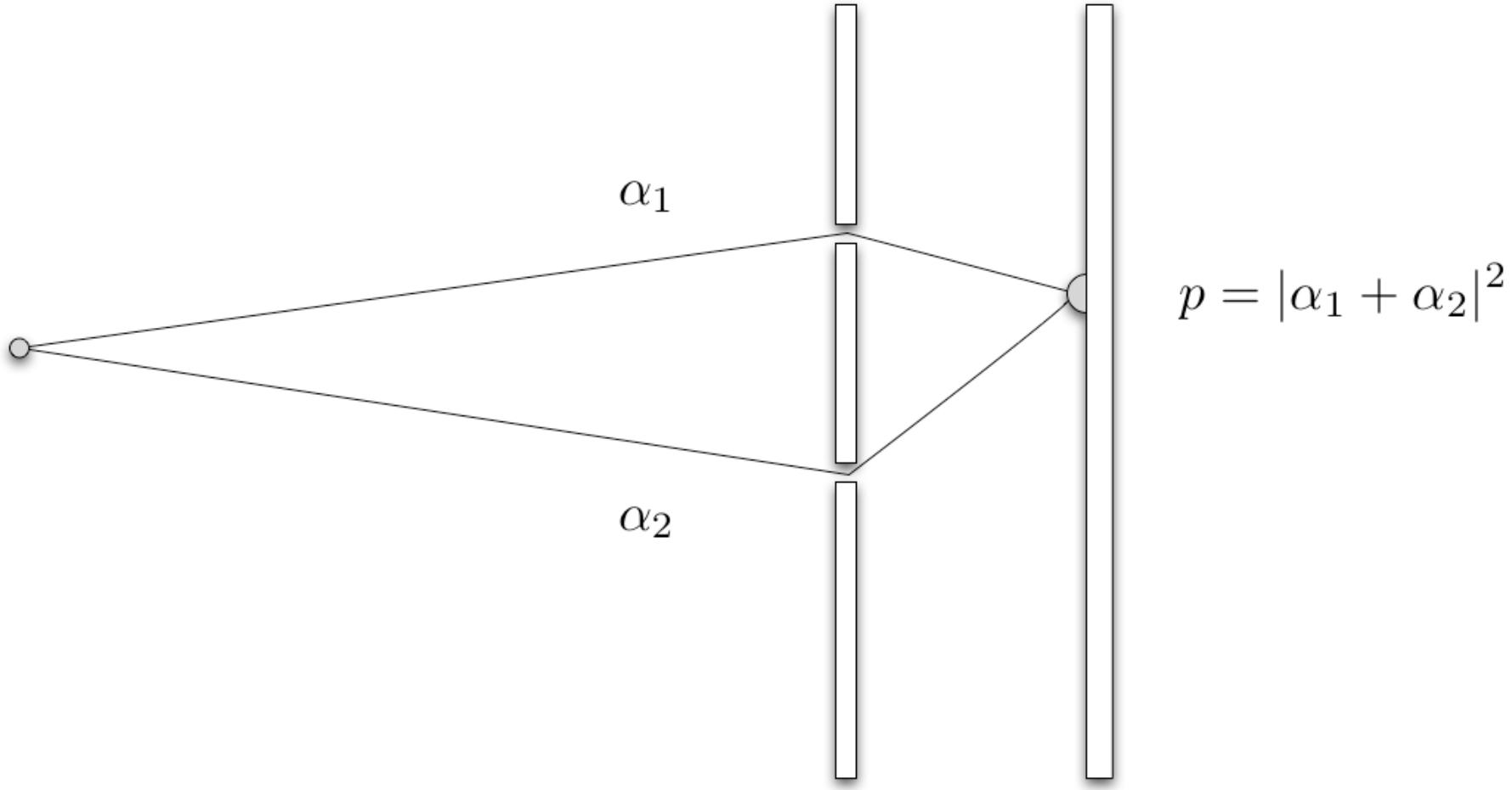
1926

† This report was originally intended for *die Naturwissenschaften*, but could not be accepted there for lack of space. I hope that its publication in this journal [*Zeitschrift für Physik*] does not seem out of place [M.B.].

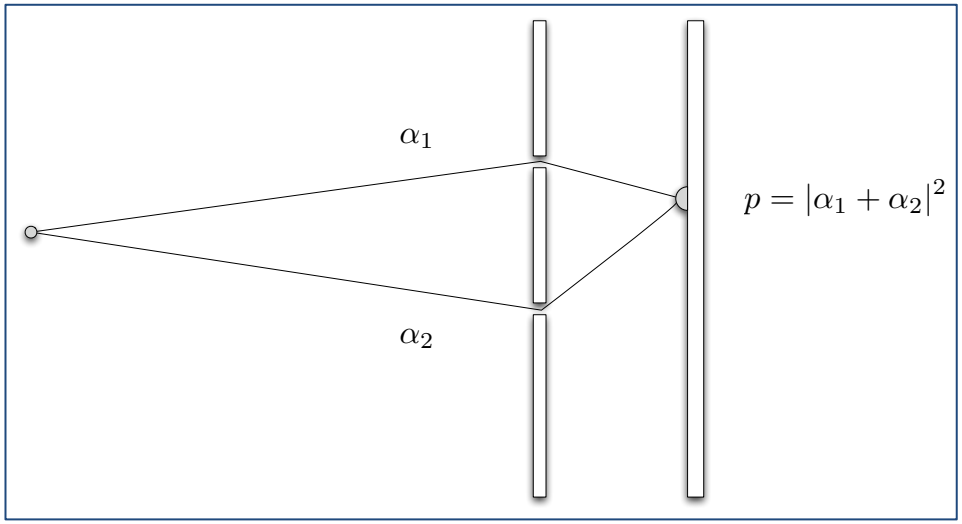
If one translates this result into terms of particles, only one interpretation is possible. $\Phi_{n,m}(\alpha, \beta, \gamma)$ gives the probability* for the electron, arriving from the z-direction, to be thrown out into the direction designated by the angles α, β, γ, with the phase change δ. Here its energy τ has increased by one quantum $h\nu^0_{nm}$ at the

* Addition in proof: More careful consideration shows that the probability is proportional to the square of the quantity $\Phi_{n,m}$.

Add amplitudes not probabilities



Quantum interference



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

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

$$|\alpha_1 + \alpha_2|^2 = |\alpha_1|^2 + |\alpha_2|^2 + \alpha_1 \alpha_2^\star + \alpha_1^\star \alpha_2$$

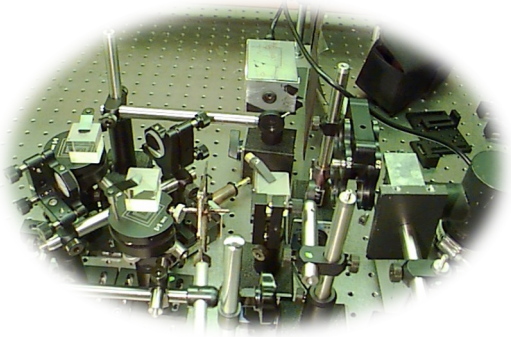
$$= \quad p_1 \quad + \quad p_2 \quad + 2|\alpha_1||\alpha_2| \cos(\varphi_1 - \varphi_2)$$

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

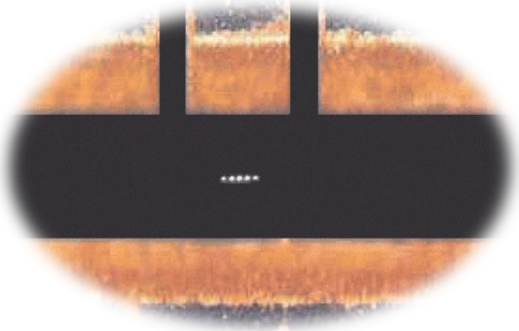
Quantum world is somewhat different…

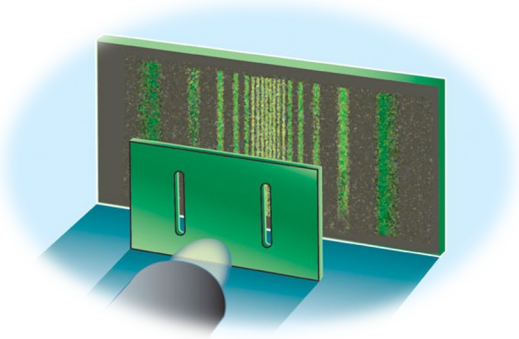
Ubiquitous quantum interference

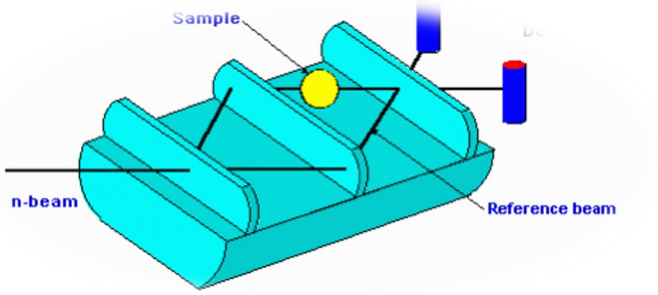
PHOTONS



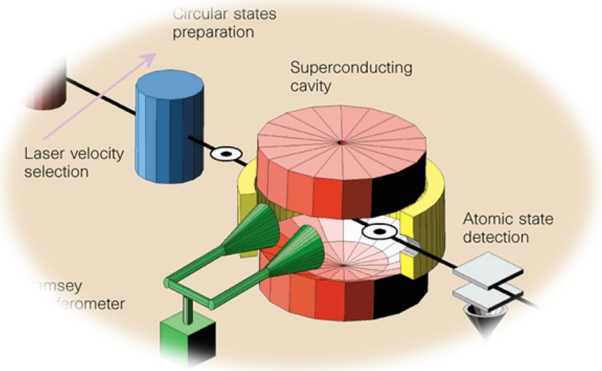
IONS





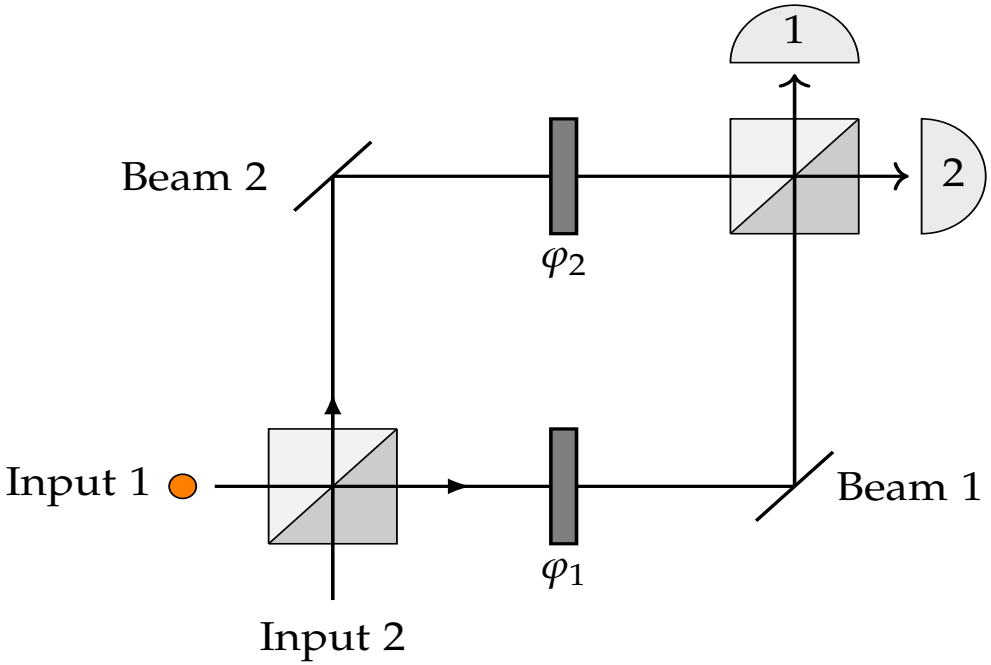


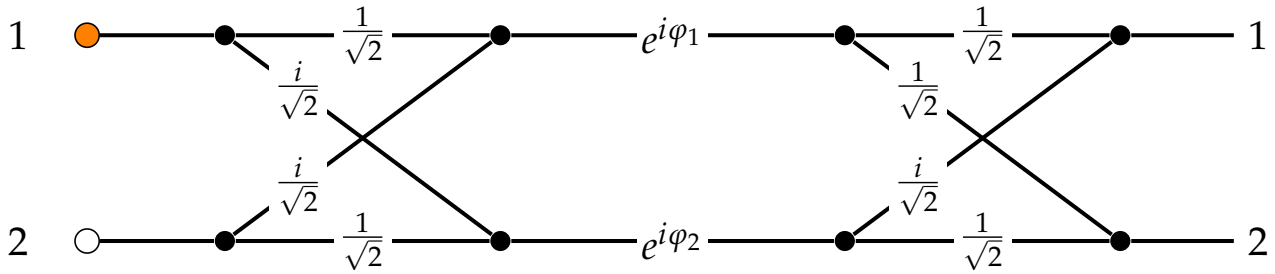
NEUTRONS



ATOMS

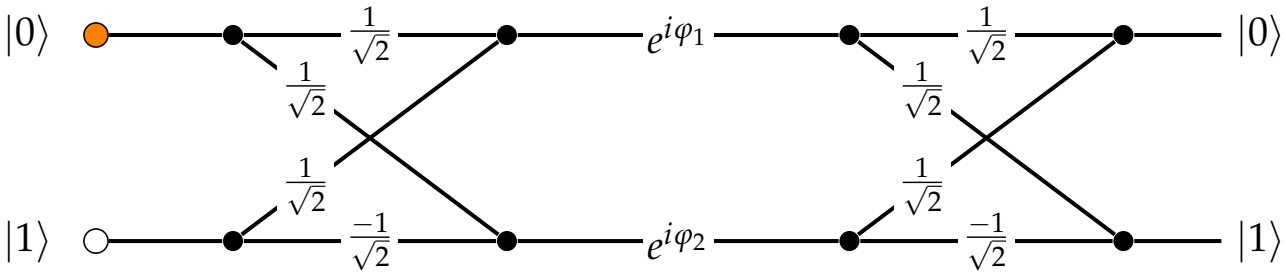
Mach-Zehnder interferometer

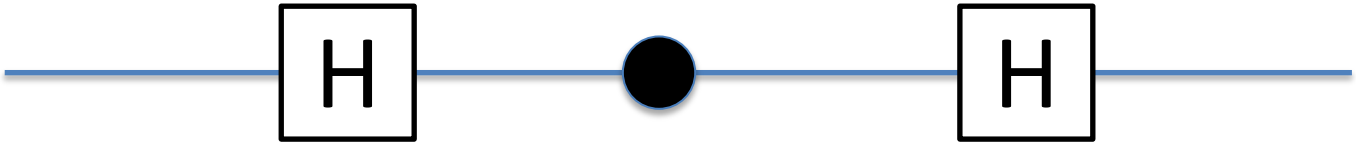




first beamsplitter phase shifts second beamsplitter

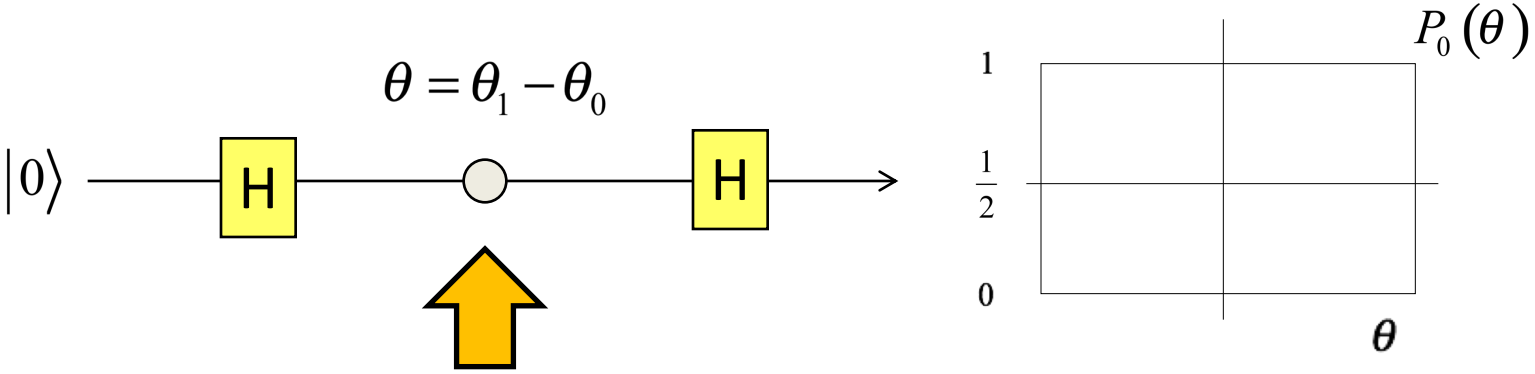
In terms of gates and circuits…





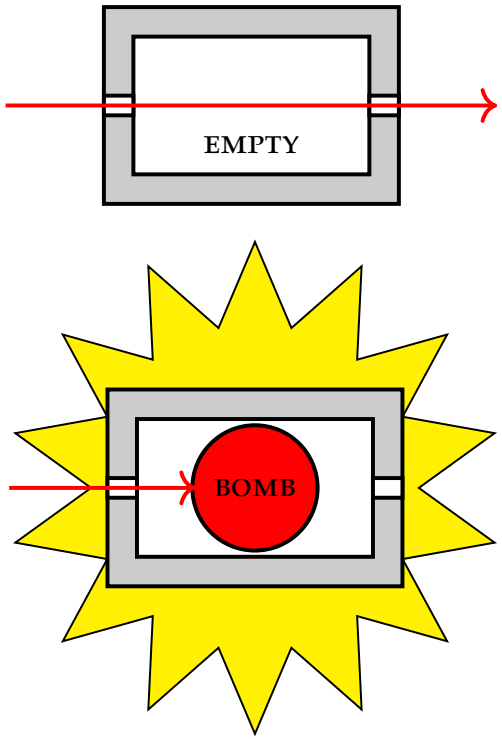
$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} e^{i\varphi_0} & 0 \\ 0 & e^{i\varphi_1} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix}$$

Quantum gravitometers, acelerometers

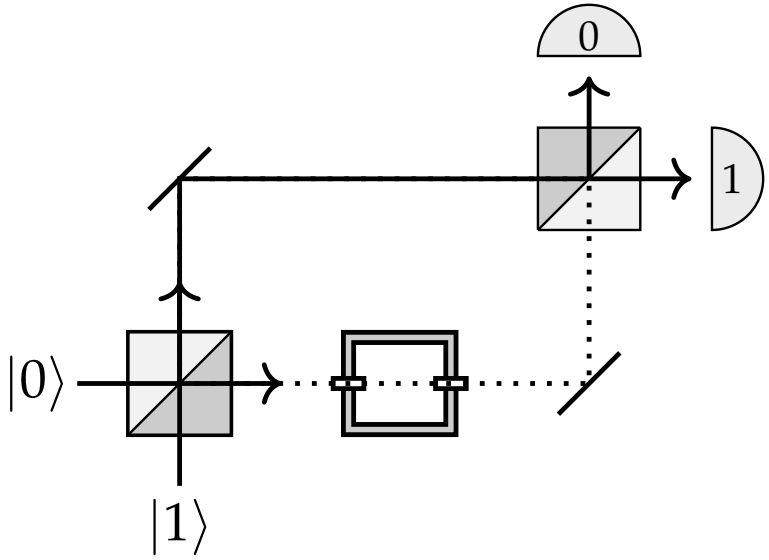


- Accelerations
- Rotations
- Laser frequency detuning
- Laser phase
- Photon recoil
- Electric/magnetic fields
- Interactions with atoms and molecules

Can you detect super-sensitive bombs?

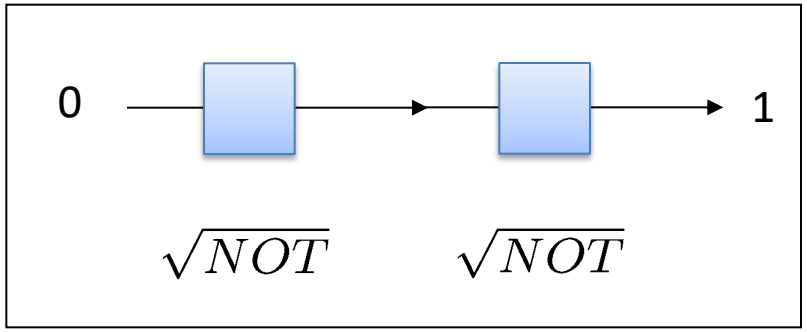


Hint: Consider the setup where the input and output ports are hooked up in one of the arms of a Mach-Zehnder interferometer.

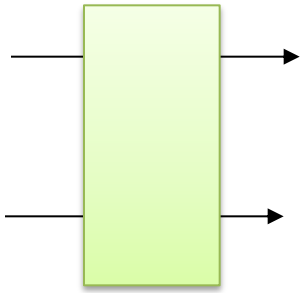


Logically impossible gates

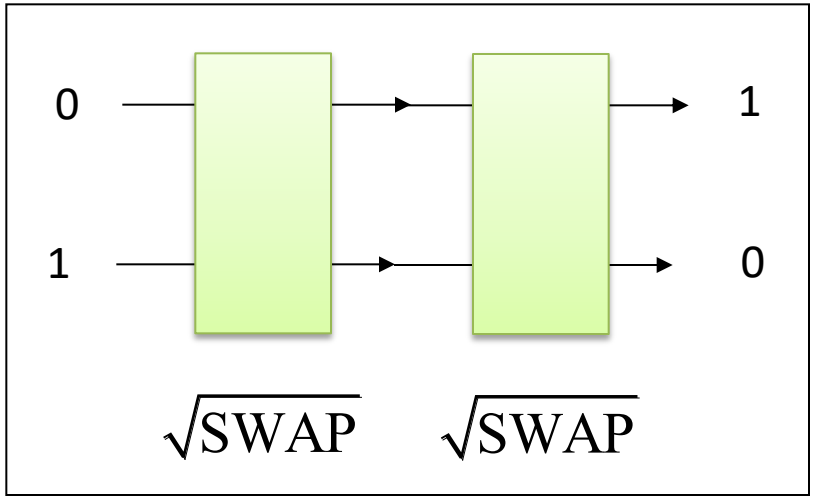
$\sqrt{NOT}$



NOT

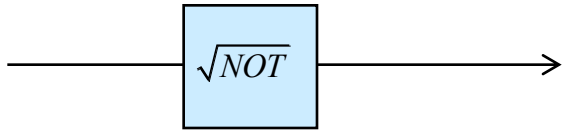


$\sqrt{\text{SWAP}}$



SWAP

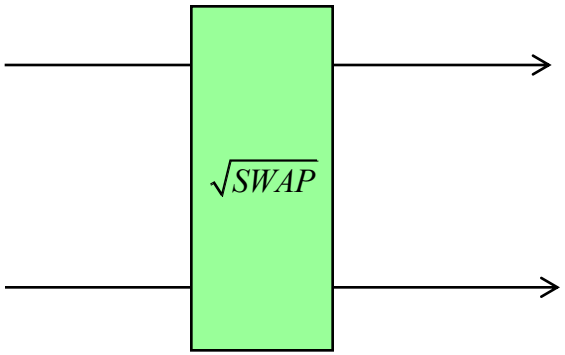
This is all we need…



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

Generates superpositions

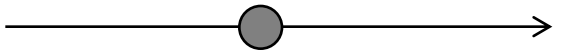
$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + i|1\rangle\right)$$



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

Generates entanglement

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

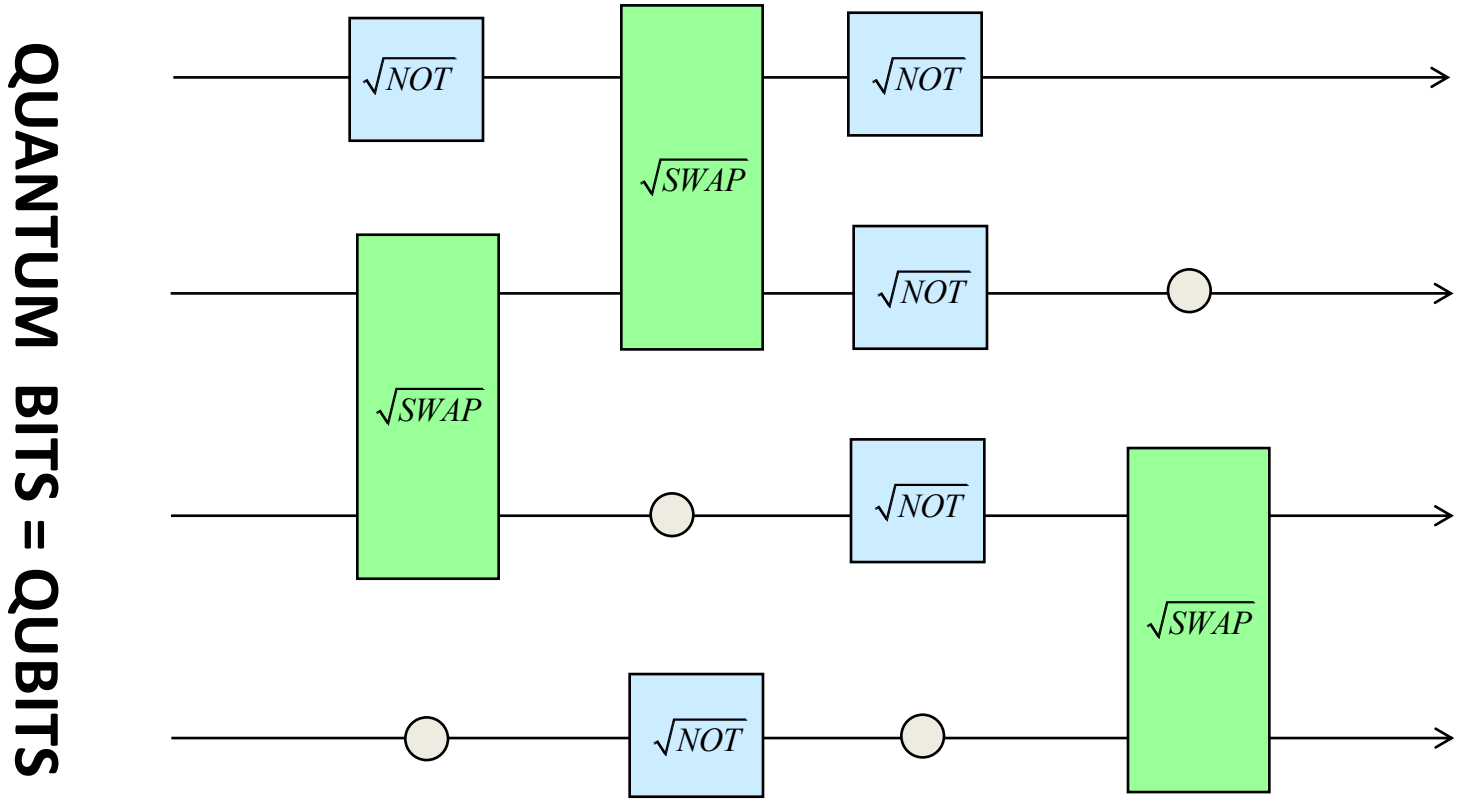


$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$$

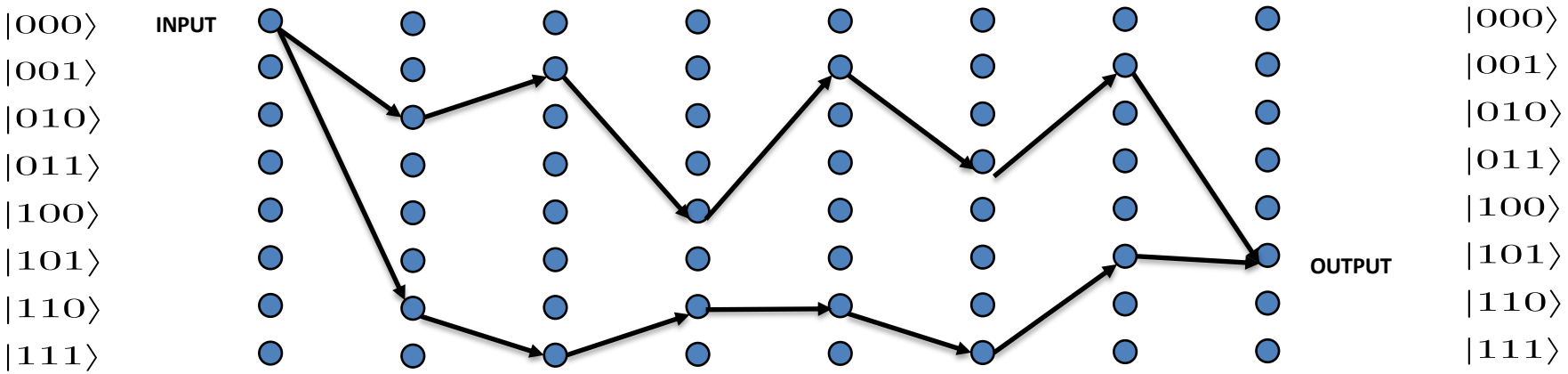
Innocuous phase gate which makes all the difference

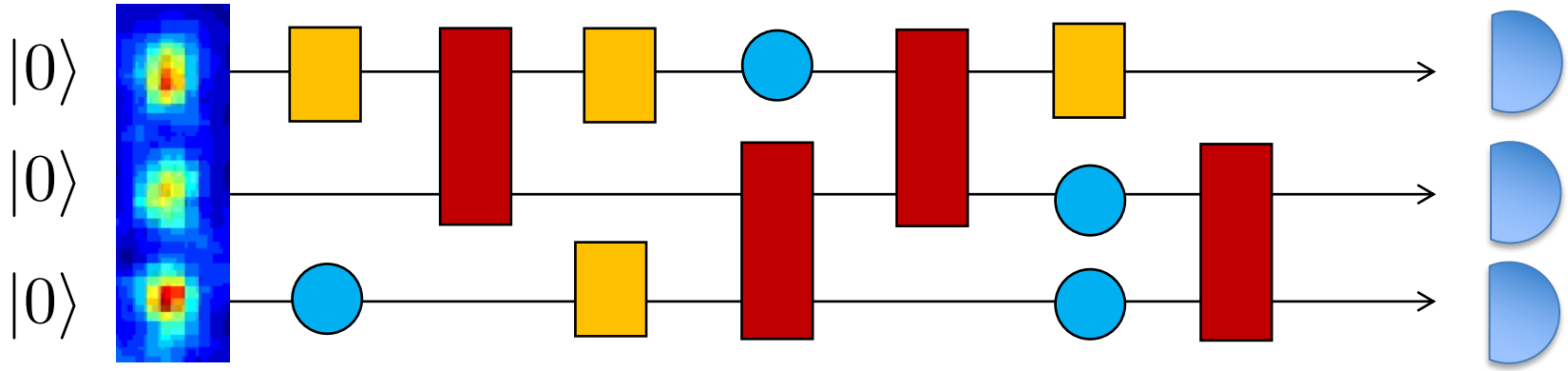
$$|0\rangle \rightarrow |0\rangle \quad |1\rangle \rightarrow e^{i\varphi}|1\rangle$$

Quantum circuits with impossible gates

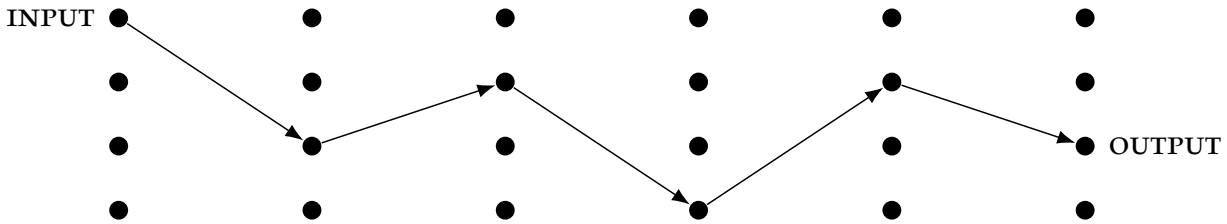


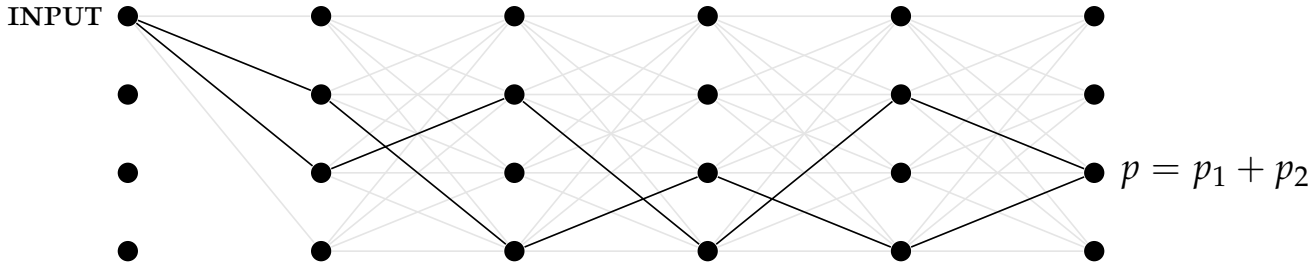
Multi-particle interference (quantum computation)

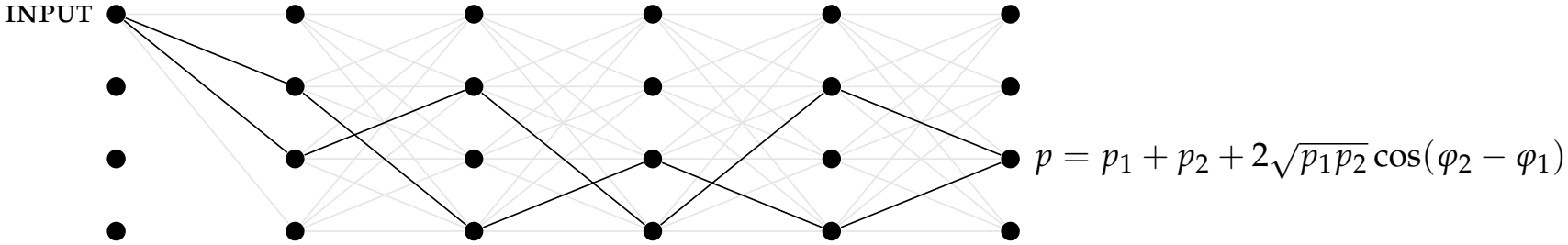




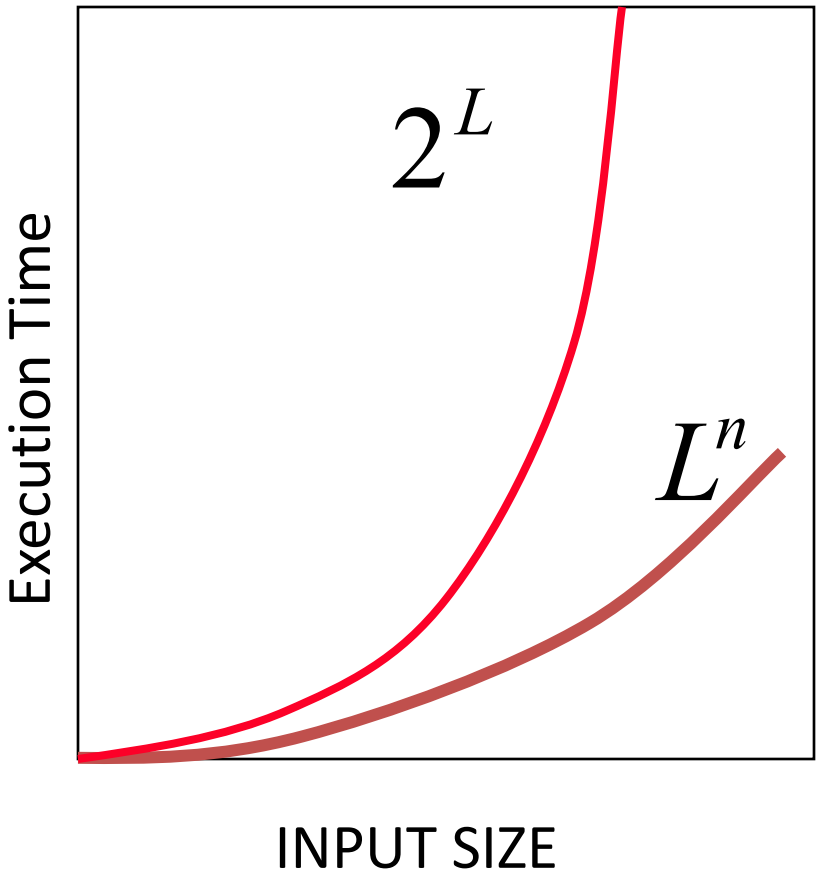
Deterministic, probabilistic and quantum

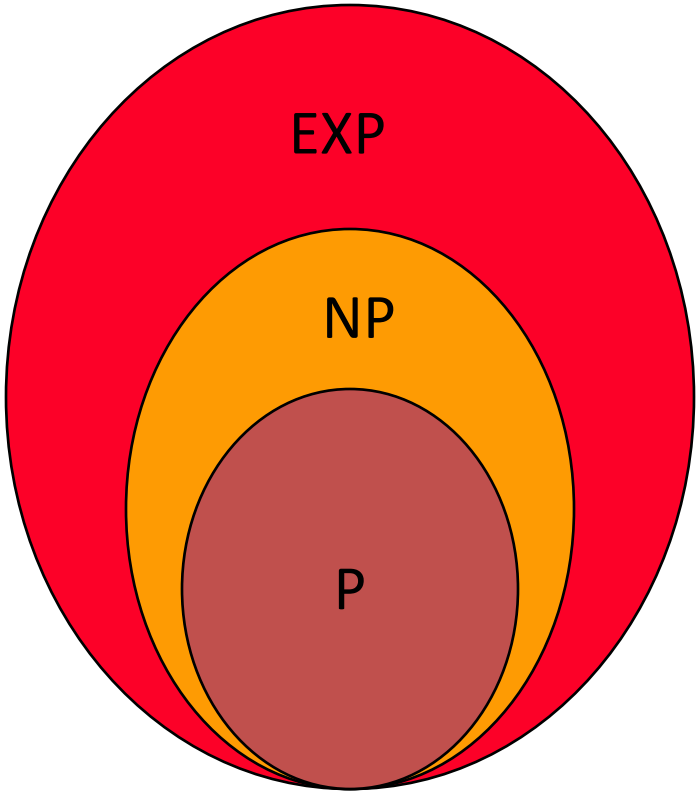




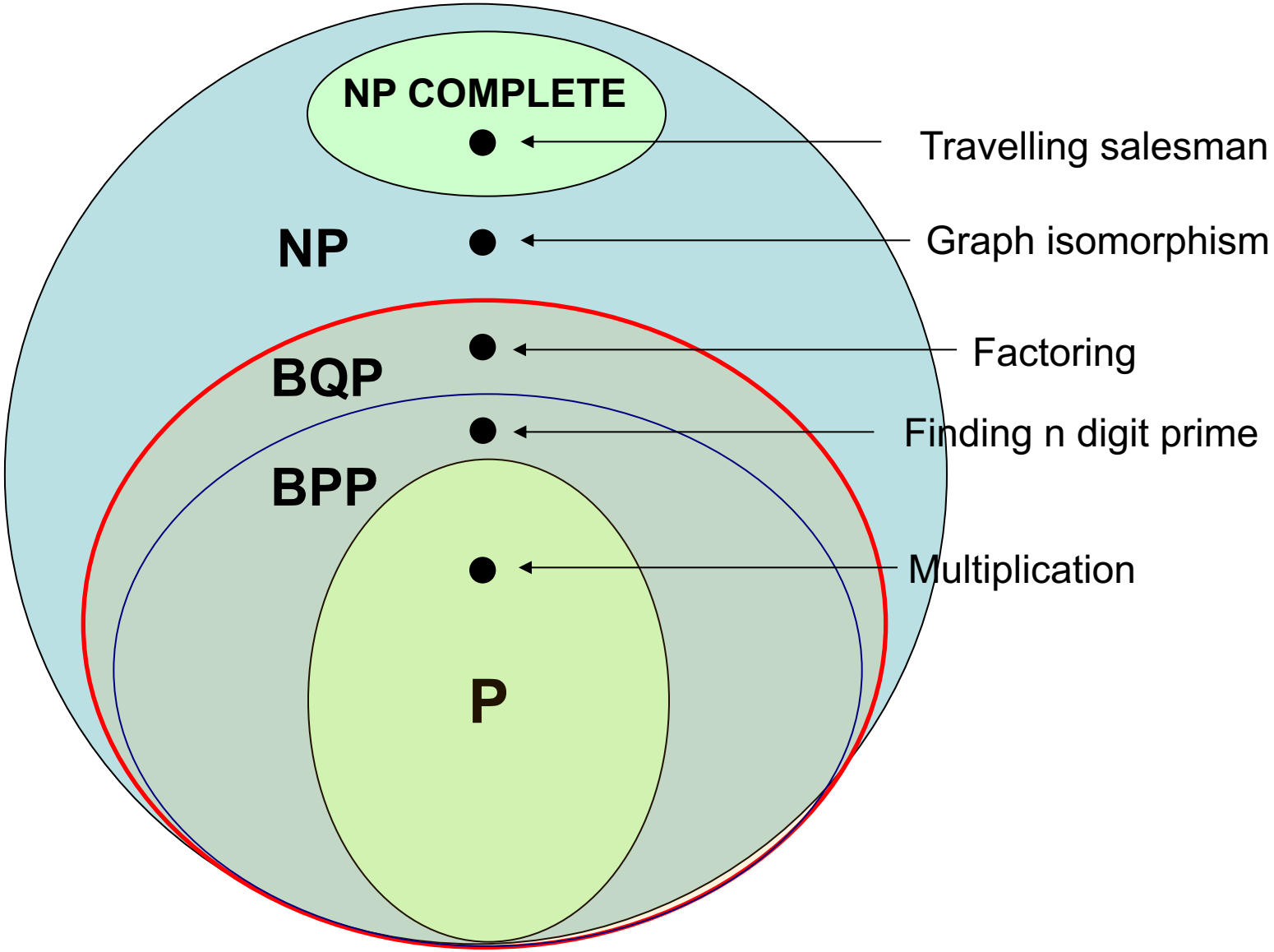


Hard and easy…



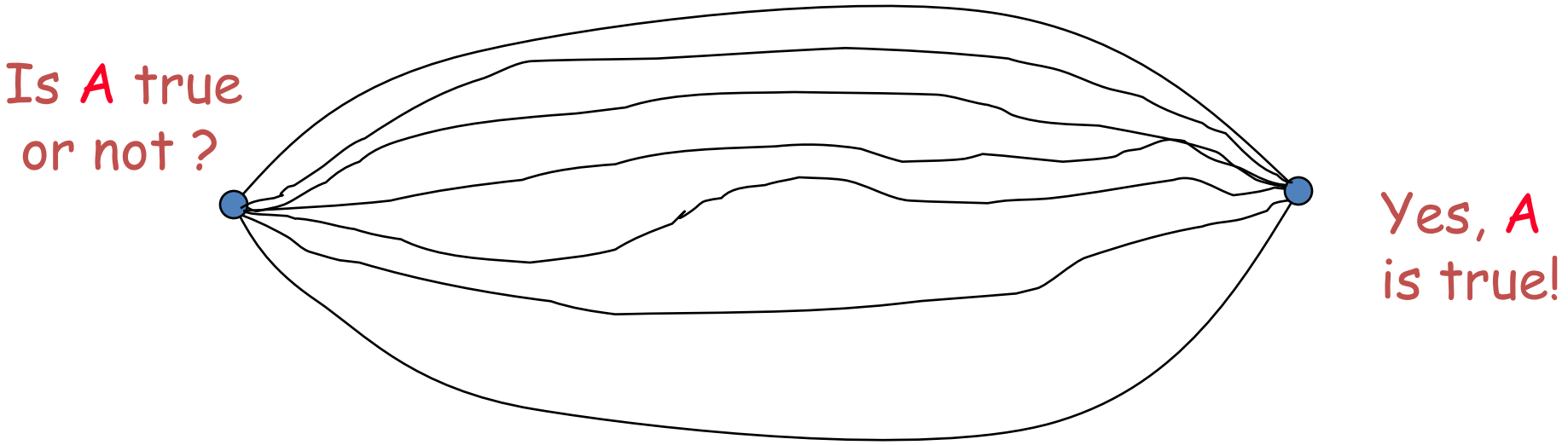


Zoo of computational complexity



Impact on logic…

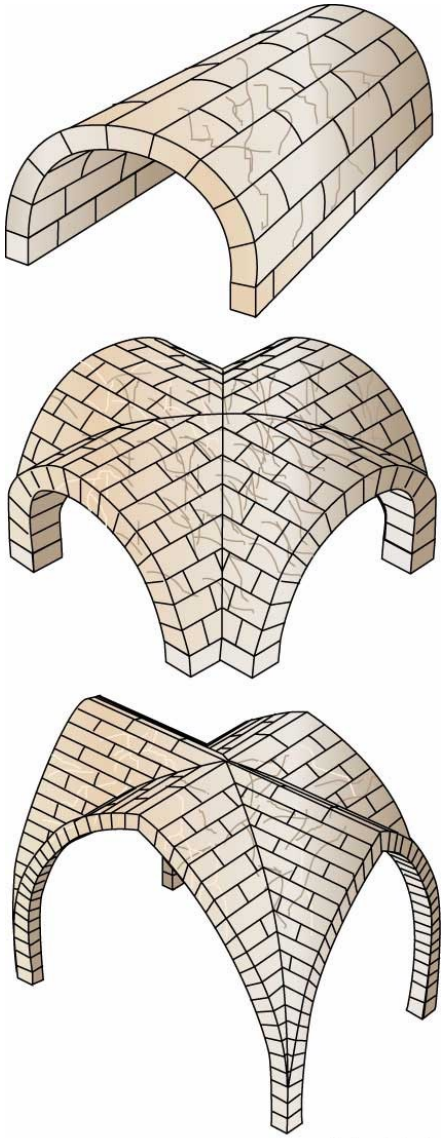
Traditional approach: proof = physical record



Testing 10^{100} different possibilities in quantum superpositions

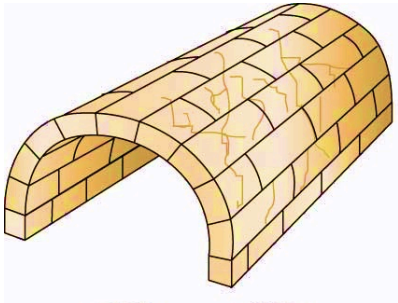
Proof = physical process

Limits to quantum computation ?

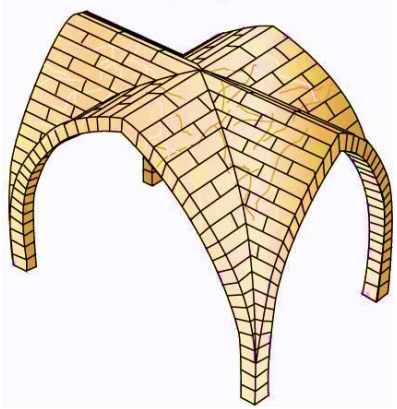


Building quantum computers…

Basic blocks

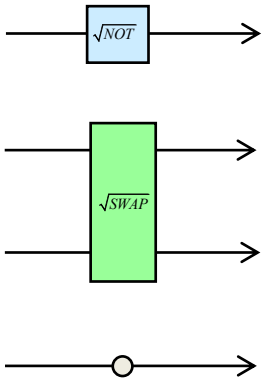


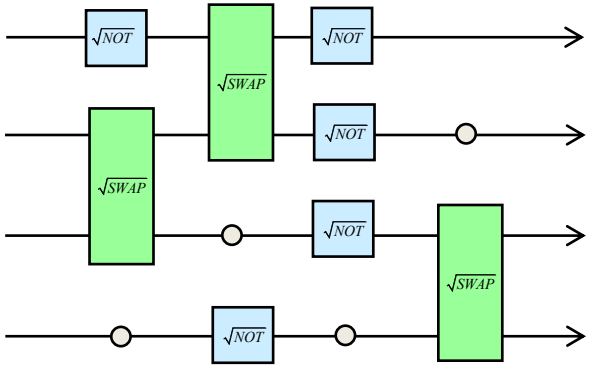
Stable &
fault tolerant

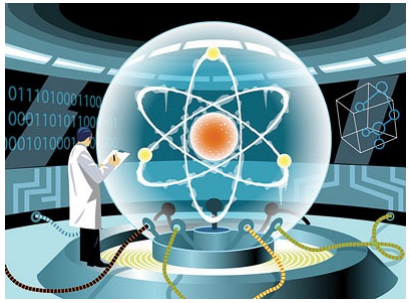


Scaling up

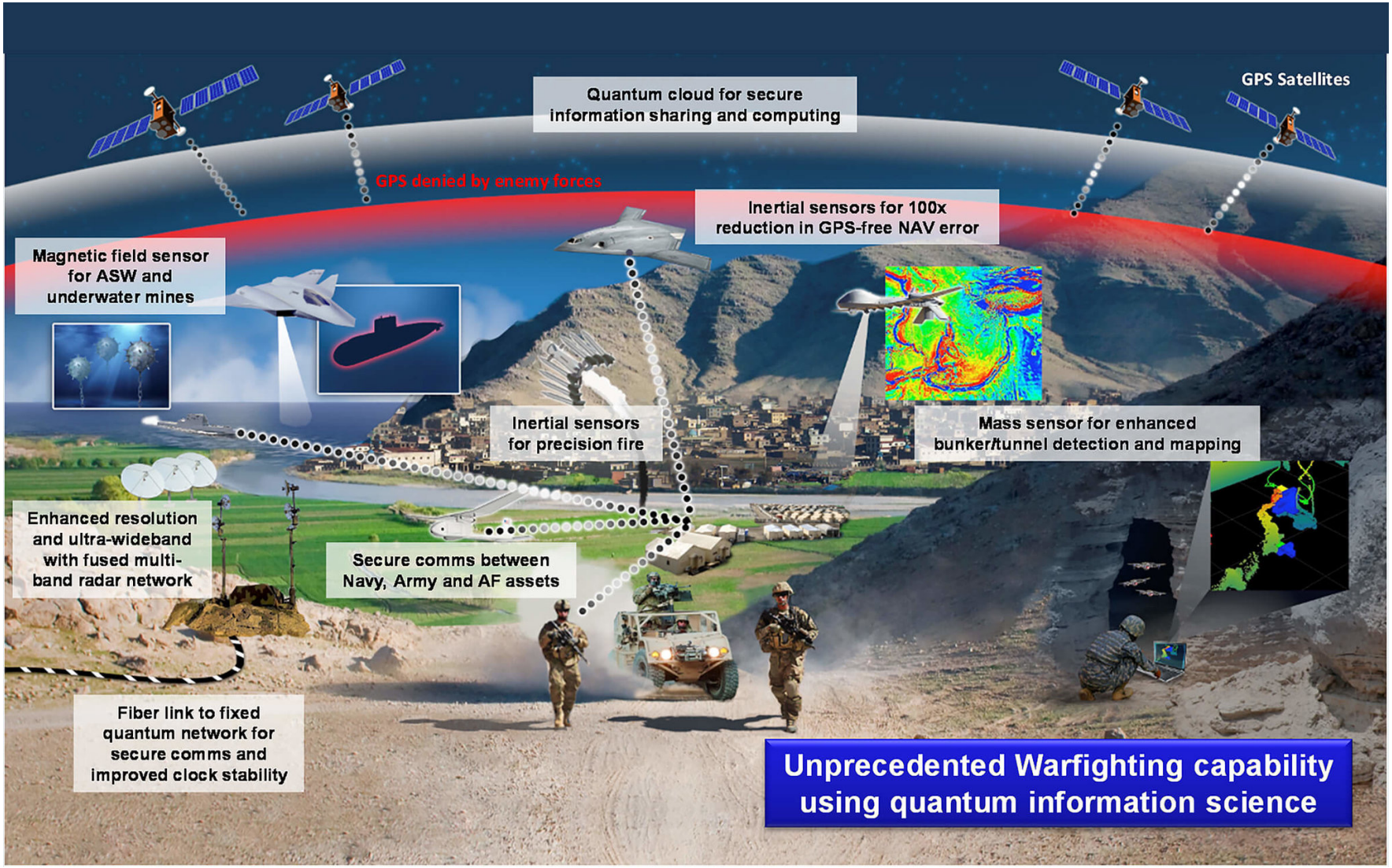
The final thing



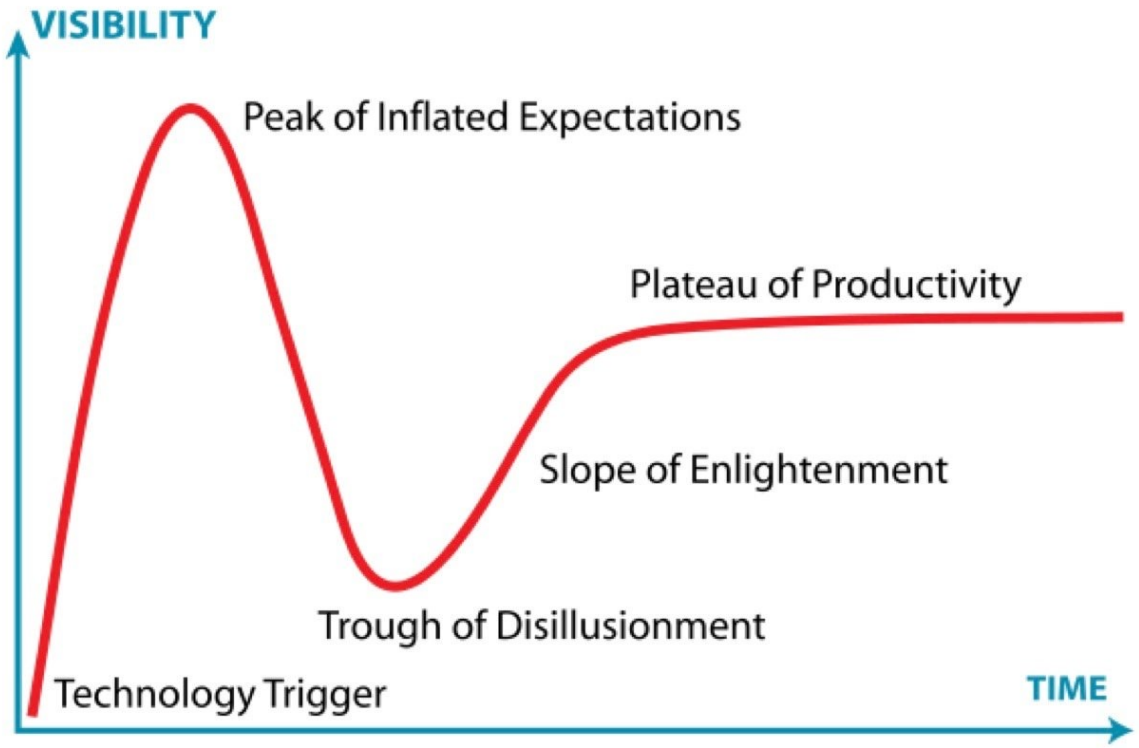




Optimists – quantum advantage

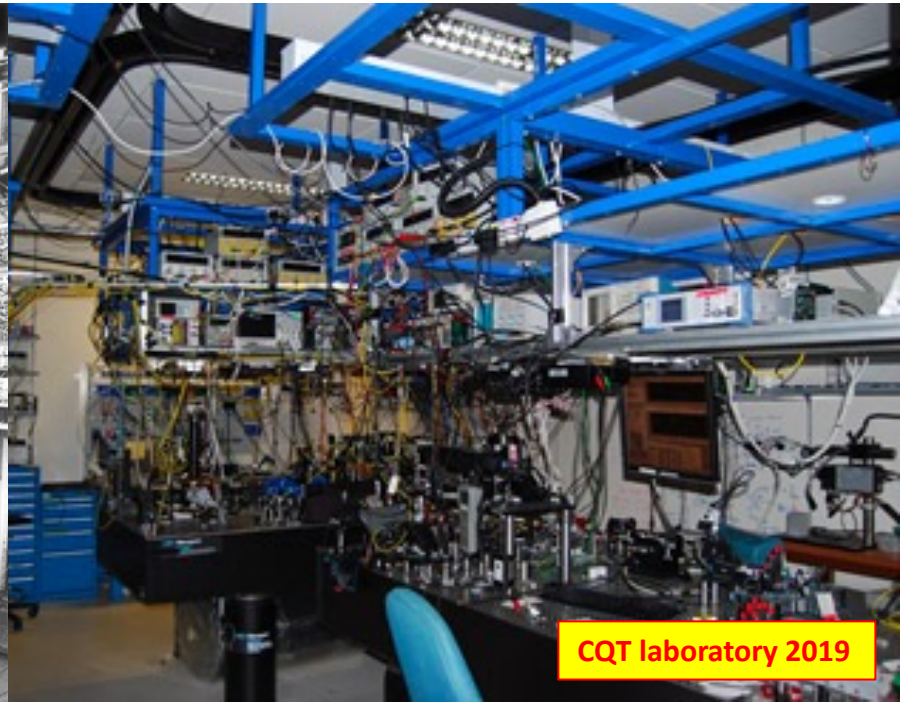


Pessimists - the Gartner Hype Cycle



Humans are famously bad at predicting the future of technologies.

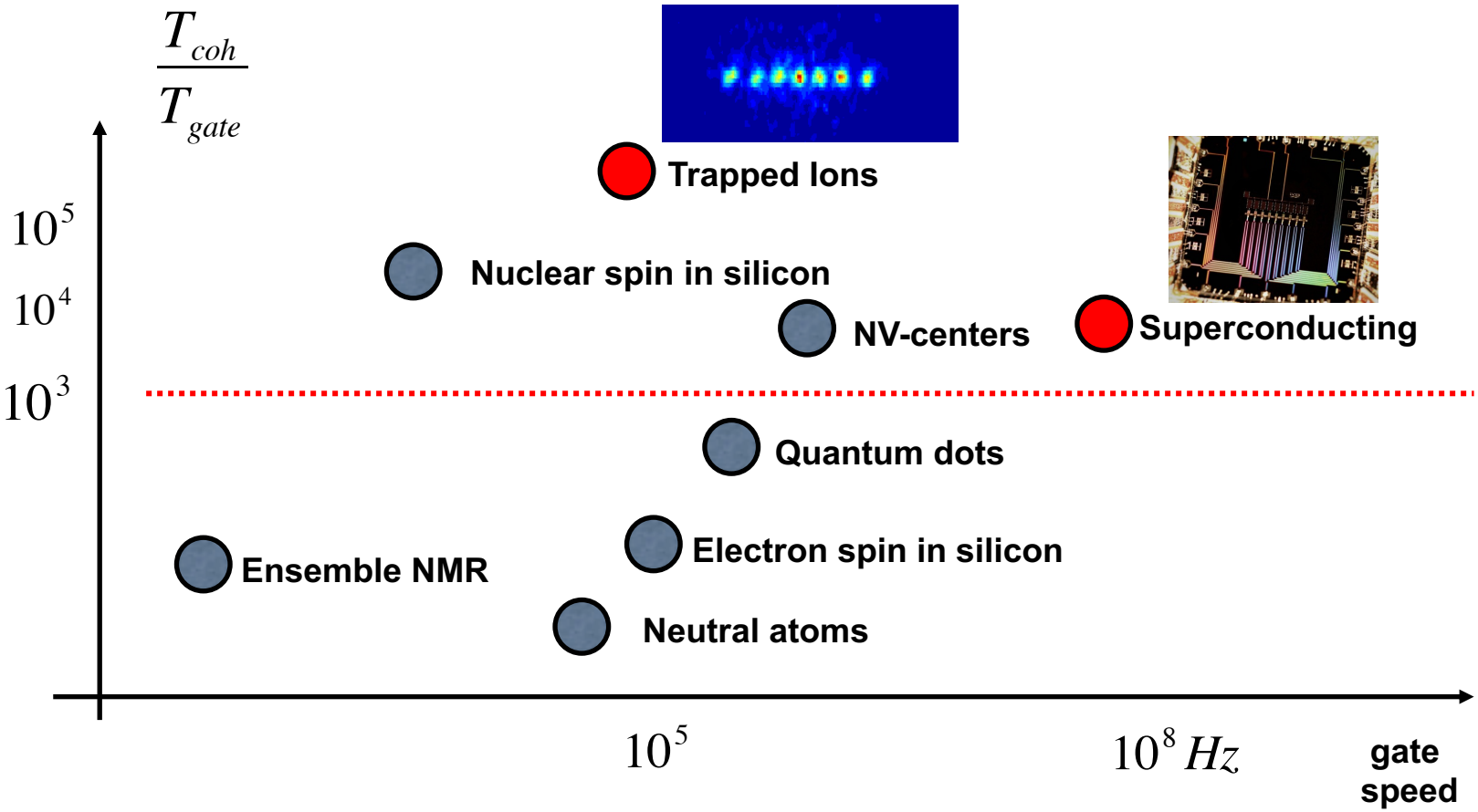
Computers & Physics

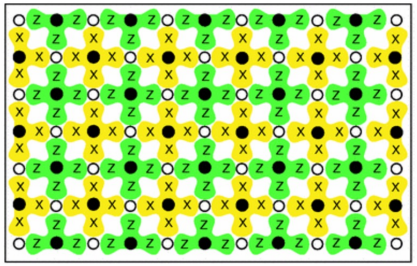


early classical computers

early quantum computers

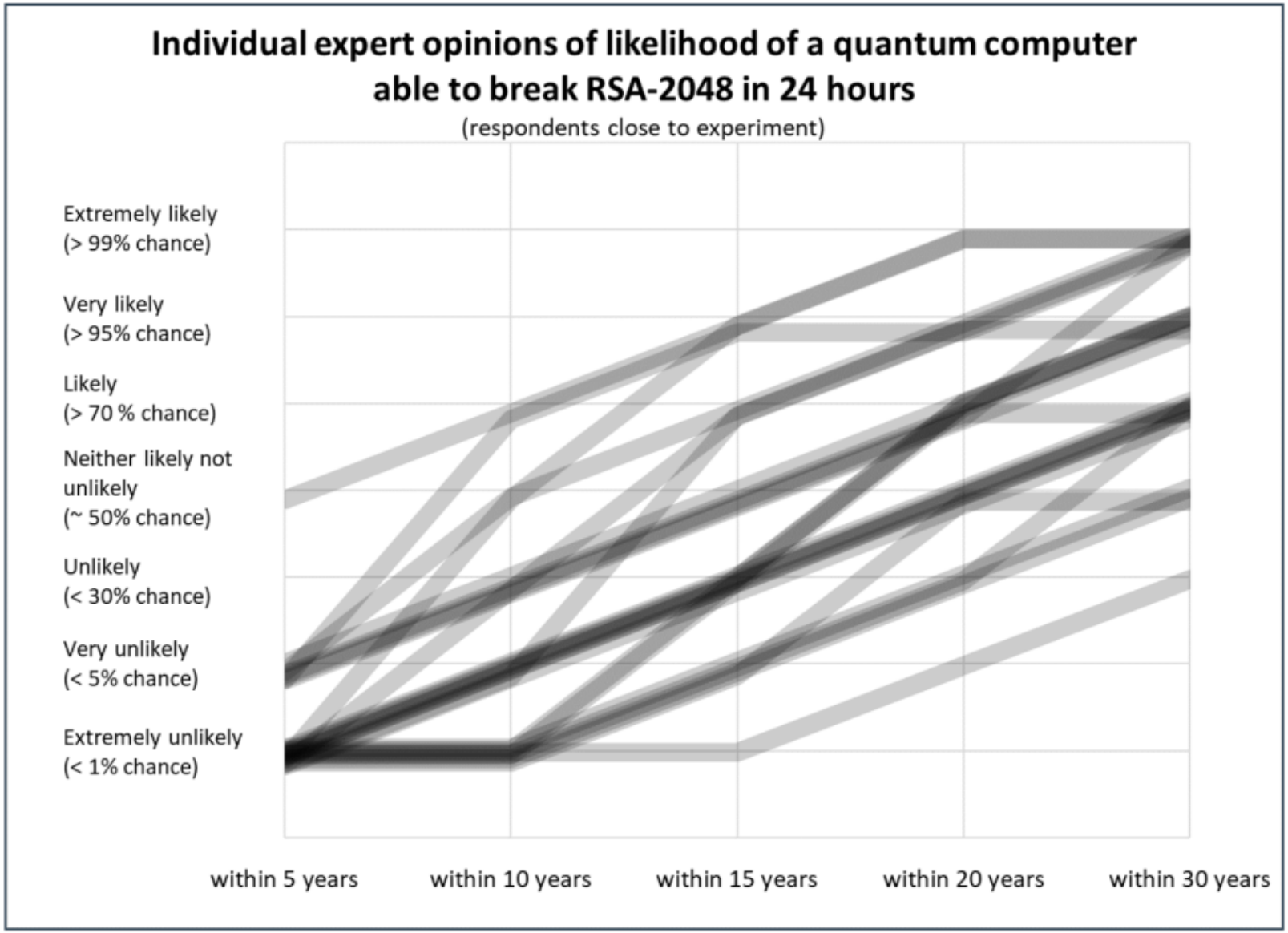
Practicalities…





quantum error correction, logical qubits, fault tolerance, scaling up

When, when, when… ?



The second quantum revolution

PRIVACY

Quantum cryptography

Secrecy based on fundamental laws of quantum physics.

Quantum internet

Distributing quantumness around the world.

PRECISION

Quantum sensing

Improving sensitivity and spatial resolution.

POWER

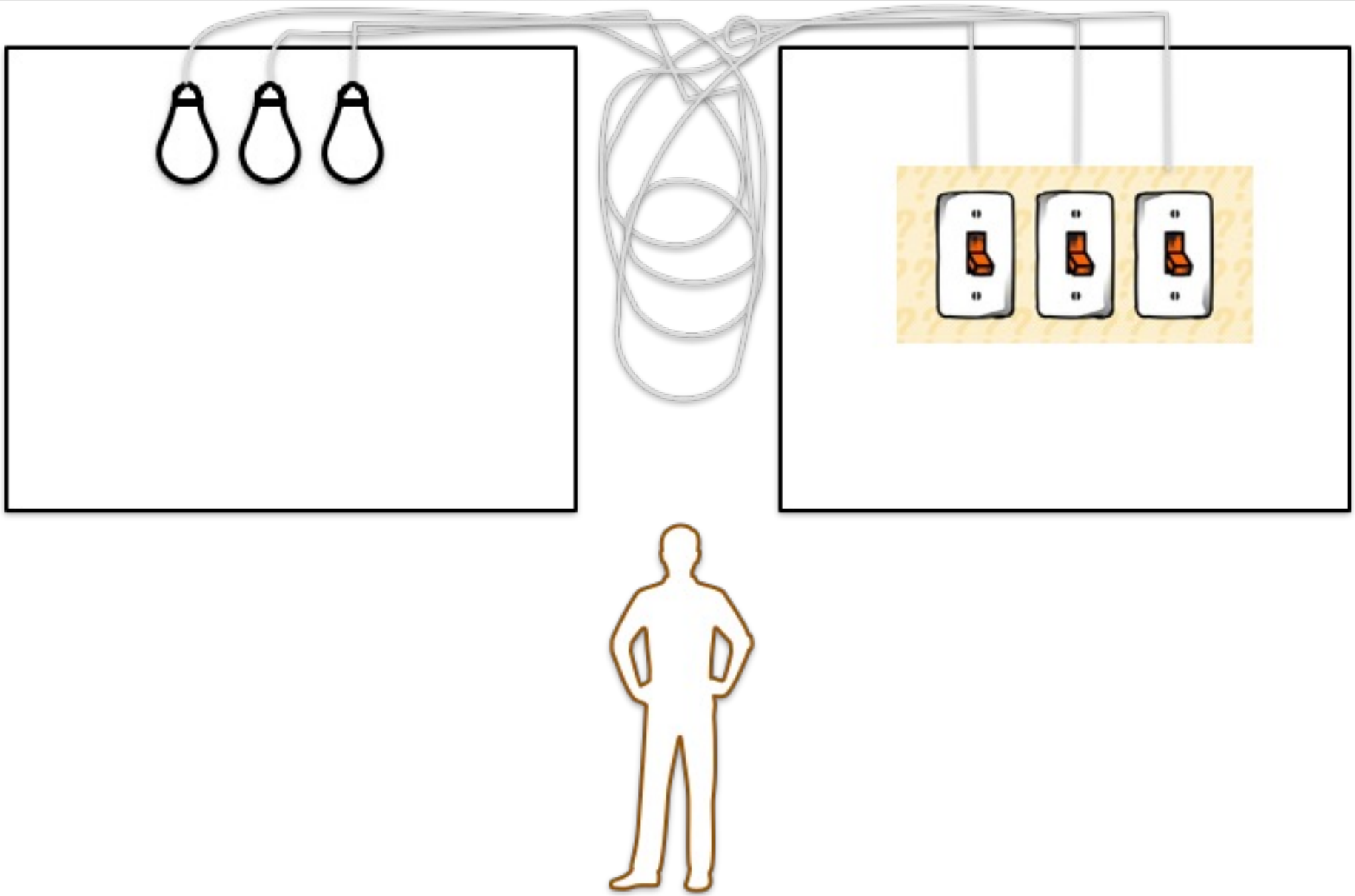
Quantum computing

New quantum algorithms for solving hard problems.

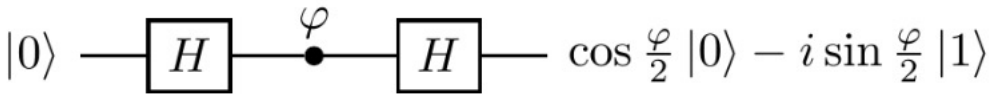
Quantum simulation

Probes of exotic quantum many-body phenomena.

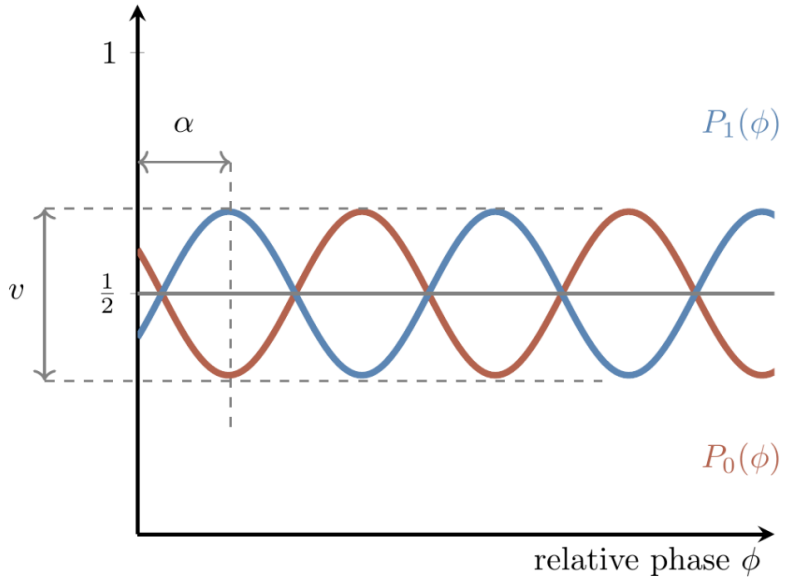
Think like a physicist



Decoherence



$$|0\rangle|e\rangle \longmapsto |0\rangle|e_{00}\rangle$$
$$|1\rangle|e\rangle \longmapsto |1\rangle|e_{11}\rangle$$



$$\begin{aligned}
|0\rangle|e\rangle &\xmapsto{H} \Big(|0\rangle + |1\rangle\Big)|e\rangle \\
&\xmapsto{\phi} \Big(|0\rangle + e^{i\phi}|1\rangle\Big)|e\rangle \\
&\xmapsto{\times} |0\rangle|e_{00}\rangle + e^{i\phi}|1\rangle|e_{11}\rangle \\
&\xmapsto{H} |0\rangle\Big(|e_{00}\rangle + e^{i\phi}|e_{11}\rangle\Big) + |1\rangle\Big(|e_{00}\rangle - e^{i\phi}|e_{11}\rangle\Big).
\end{aligned}$$

$$P_0(\phi) = \frac{1}{2}\big(1 + v\cos(\phi+\alpha)\big),$$
$$P_1(\phi) = \frac{1}{2}\big(1 - v\cos(\phi+\alpha)\big).$$

Turning the tables on decoherence

"The mind adapts and converts to its own purposes the obstacle to our acting. The impediment to action advances action. What stands in the way becomes the way."

Marcus Aurelius' *Meditations* 5.20