



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?

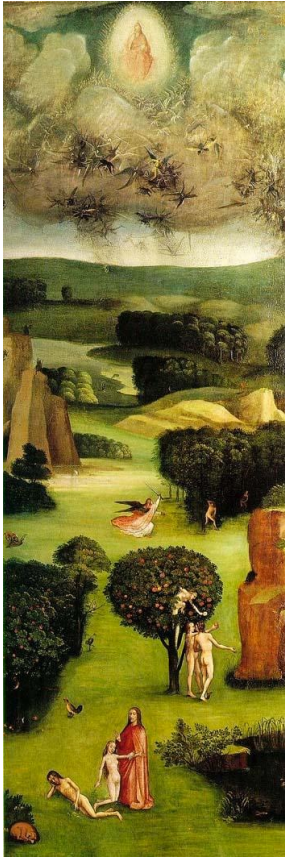
**EPICURUS
(300 BC)**

**DEMOCRITUS
(400 BC)**

atoms *swerve* at
random along
their paths

atoms follow
predetermined paths

Determinism, free will & moral responsibility



The Last Judgement, Hieronymus Bosch (1482)

More pragmatic approach - gambling



Caravaggio, *The Cardsharps* c. 1594

Girolamo Cardano - Gambling Scholar

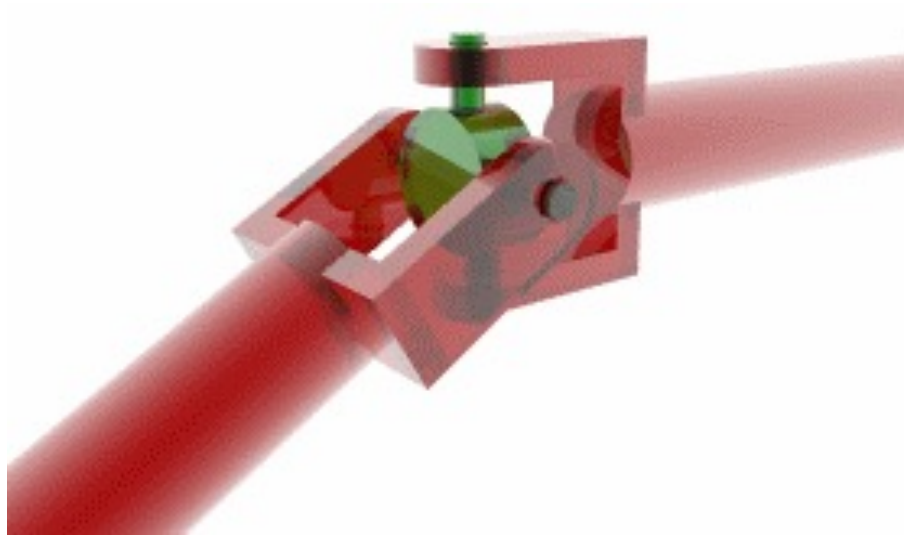


1501-1576

Cardano described himself as

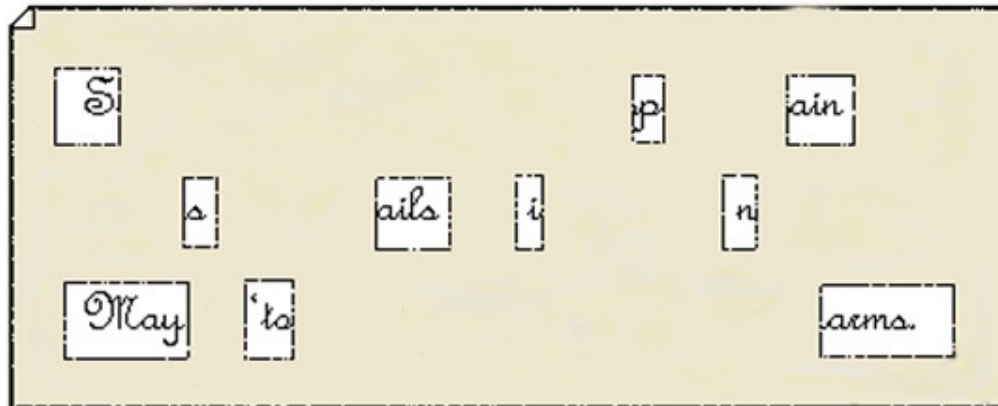
Hot-tempered, single-minded, and given to women, ...cunning, crafty, sarcastic, diligent, impertinent, sad, treacherous, magician and sorcerer, miserable, hateful, lascivious, obscene, lying, obsequious,...fond of the prattle of old men.

Cardano's shaft joint



Cardano's grille

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



Probability and complex numbers

De ludo Aleæ Liber. 265

CAPVT XIII

De Numeris compositis, tam vsque ad sex, quam ultra, & tam in duabus Aleis, quam in tribus.

IN duabus Aleis duodecim, & vdecim consistant eadem ratione, qua bis, sex, atque sex, & quinquæ. Decem autem ex bis quinq; & sex, & quinq; hoc autem variatur dupliciter, utiq; totum duodecim pars circitum, & sexta æqualitas. Restum ex novem, & quinq; & quinq; & sex, ac tribus, vt in ista pars circitum æqualitas duplum nome parti. Ocho autem puncta sunt ex bis quinq; tribus, & quinq; & sex, & tribus. Totum quinq; septima sunt circitum pars, & diæ septima æqualitas. Septem autem, & sex, & sex, & quinq; ac duabus quinq; ac tribus. Omnia iuxta puncta sunt sex, tercia pars æqualitas, & sex circitum. At sex vt octo, & quinq;, vt nouem quinq; vt decem, tria vt vdecim, & duo vt duodecim.

Sed in Ludo sitilli vdecim puncta, adde decem, quia vna Alea potest offerri etiam igitur duobus punctibus istum duodecim, & ita bis æqualitas, & trius circitum. Tria autem restum, quinq; autem quatuordecim, quinq; quinquodenis, duabus æqualitas, & à toto circitum quinq; ac sex. Sex autem sexdecim, & vnde præp æqualitates.

Contentis fortis in duabus Aleis.

2	12	1	3	11	2	4	10	1
3	9	4	6	8	5	7	8	4
4	18	1	4	13				
5	16	6	6	13				
6	15	10	6	13				
7	14	15	8	10				
8	13	21	9	17				
9	12	25	10	16				
10	11	27	11	18				
			12	16				

Vna hanc numerum totidem quod in forte vt 15, 21.

Vnam punctum pectera habet tot. Duo puncta habent 11.

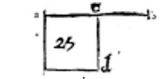
In tribus autem Aleis tria puncta. Septem sequitur æqualitas in Fortis, vt forte puncta ad viginti. Singuli autem numeri per se in vna Alea proportionem habet subtriplo, cum ergo tres sint Aleæ obiciuntur proportionem æqualitatis, vt ex duobus sedecim consistuntibus, singula puncta in octo, & octo interuenit, & in totidem non interuenit, vt sit ratio hæc ad viginti, vt vna puncta in duabus Aleis ad totum circitum in tribus sitibus, vel in dimidio ad æqualitatem.

Tom. I.



Cap. XXXVII. De Regula falsæ. 287

In 1. pof. 1000. n. 1. pof. 1. quad. 10000. n. 1. quad. m. 200. pof. differentia 10000. n. 200. pof. æqualis 400.



his æquantur 10000. s. 1. quadrato, abier comitania, habebis 6000. æqualis 100 positionibus. igitur res est 45, & tantum habet m. 34 est debiti, & duo centi restatum ad 100. scilicet 12. igitur Franciscus habuit 48. aureos debiti, sint vero capitali vel puto, & hoc est vortu fut. 12. aureorum, & licet oportet penentes ad questionem difficultatis, ac inuestigabilis. Tã mudi etiam hæc est.

QUESTIO II. Ego habeo aureos 12. plus Franciscus, & ego meorum est, 1661. auri plus octo Franciscus, ponatur 1. res m. Franciscus, ego habeo 12. aureos m. 1. positione duæ res cubum partes, sunt 1. cubus m. & 12. s. 36. quadratus m. 144. restum m. 1. cubo, horum differentia est 1661. igitur 12. cubus m. s. 432. restum p. 1161. æquatur 1723. s. 16. quadratus m. 1. cubo, restum m. 1. cubum & 1161. ex vtraque parte, sunt 432. res æquales 36. quadratis p. 567. quæ 1. quadratum p. 1723. m. 12. cubum, igitur res est 1723. hoc habuit m. Franciscus, & ego 1707. s. & totum auri questu.

QUESTIO III. Eadem modo, si dicam quomodo sic, auri non sunt 12. s. quomodo Franciscus. Et quadratum meorum est 128. s. cubo auri m. Franciscus, debemus rem vniam m. Franciscus, ego vero habeo 12. aureos m. 1. res, & quadratum meorum est 144. s. 1. quadrata m. 36. restum, de hoc æquale est m. 1. cubo p. 1. igitur 16. s. 1. quadrato m. 1. cubo, æquatur 144. restum. Et res est 16. m. & tantum habet Franciscus debiti, ego vero aureos 8. pœuip.

QUESTIO IV. Secundum genus positionis falsæ, est per rationem 75. Et dato exemplum, si quis dicit, diuide 10. in duas partes, ex quarum vnâ in reliquam diuisa, præceditur 20. aut 40. manifestum est quod casus seu questio est impossibilis, sic tamen operabimur, vtinet ex dimidio 10. quod est 5. restatum 5. sic ut sit 5. 25. restum ex 25. addit & minor 10. restatum 15. sunt partes 7. & 1. m. haurio quadrata sunt 50. & aggregatum est 6.

QUESTIO V. Per item regulam quartæ hæc, fac ex 6. duas partes, quarum vna in reliquam duob; præcedatur m. 40. diuisum 6. in 10. si 5. addit ad 40. fit 45. maior 8. q. 8. 7. 2.

DEMONSTRATIO. Vt igitur regula venis poterat intel-

PROBABILITY Liber de Ludo Aleæ

COMPLEX NUMBERS Ars Magna

What is probability...

OBJECTIVE
FREQUENCIES

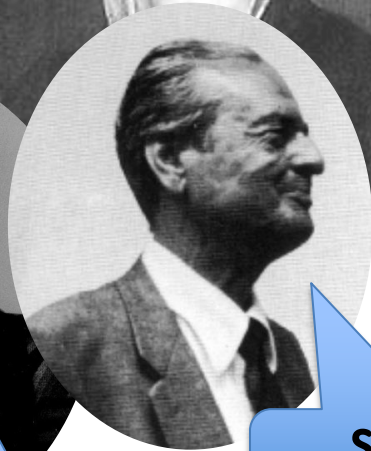
SUBJECTIVE
LACK OF KNOWLEDGE

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

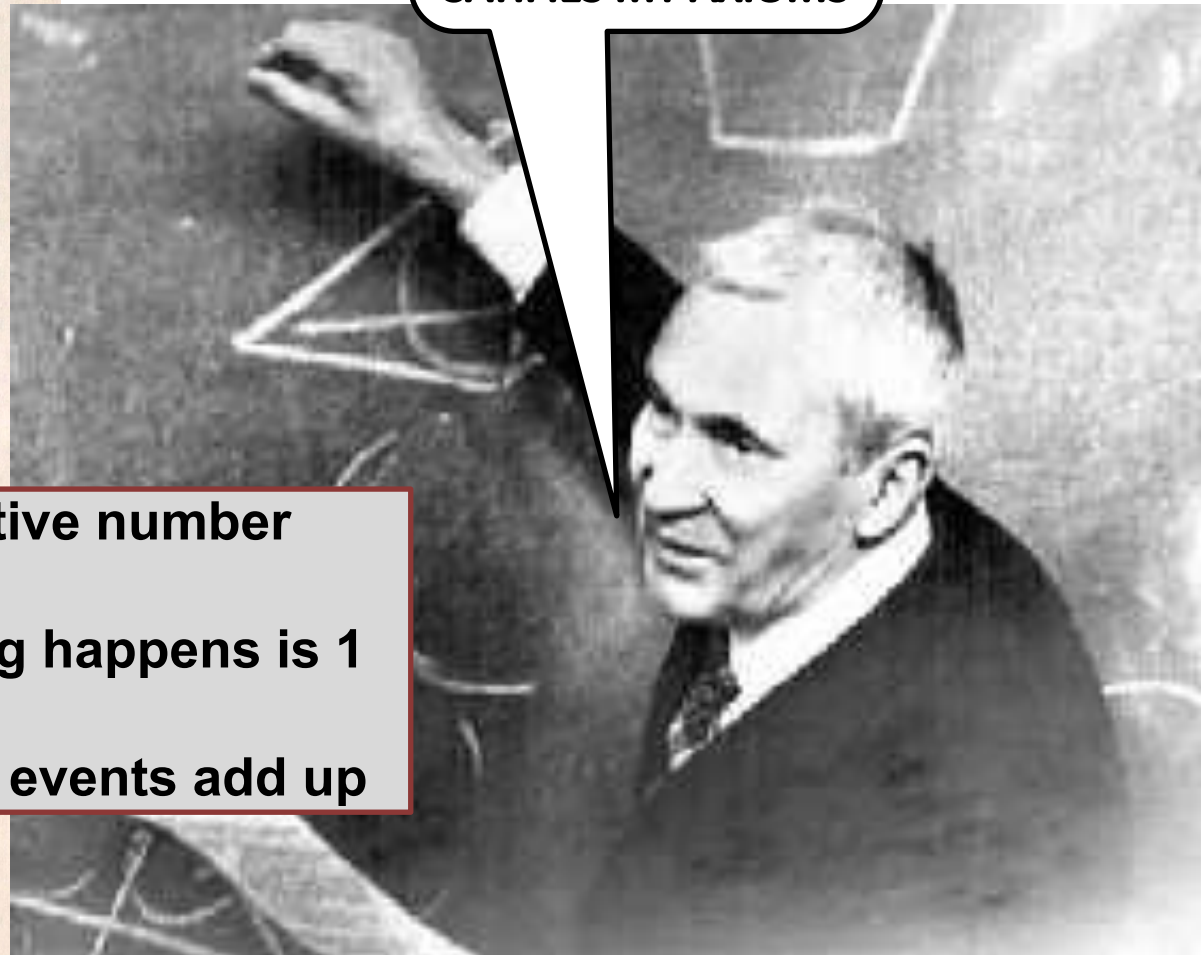
Probability is a non-negative number

Probability that something happens is 1

Probabilities of exclusive events add up

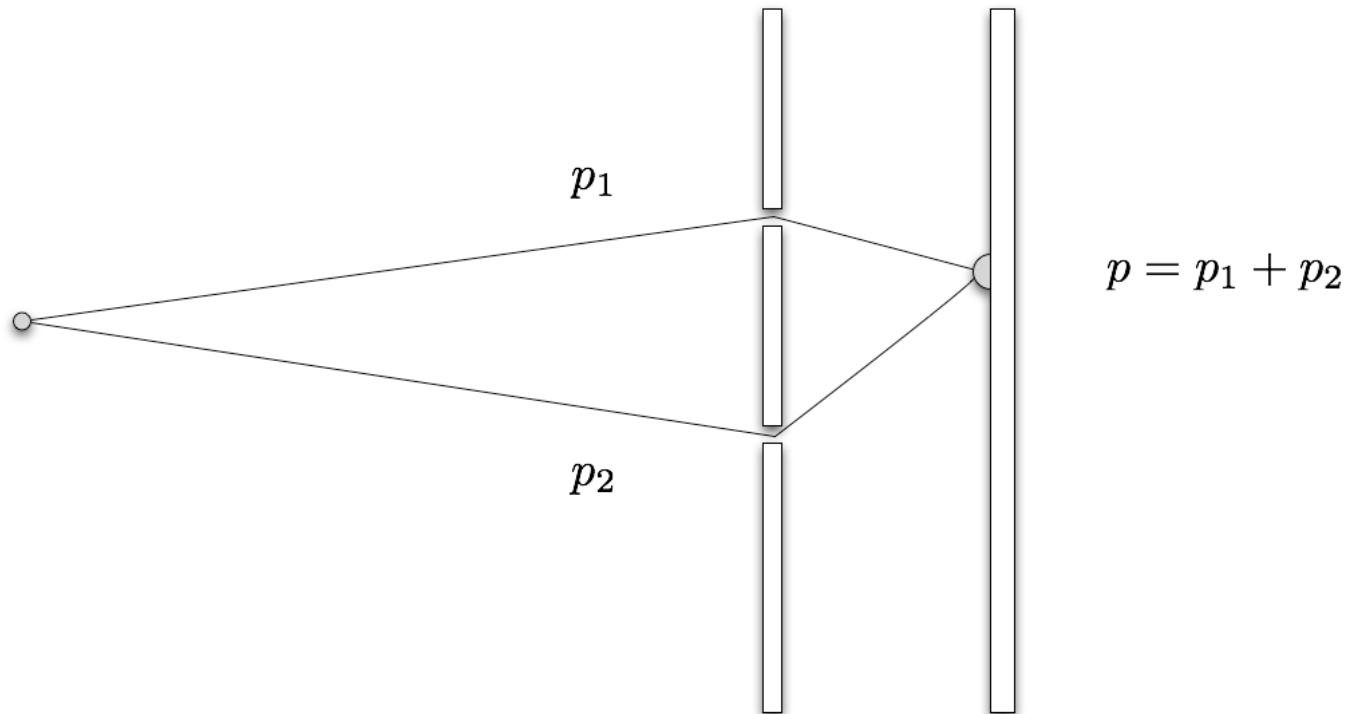
BERLIN
VERLAG VON JULIUS SPRINGER
1933

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

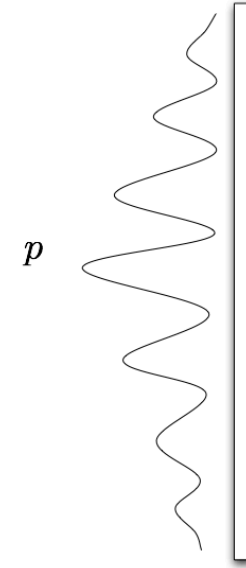
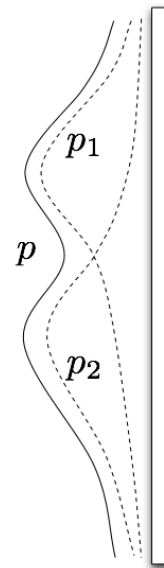
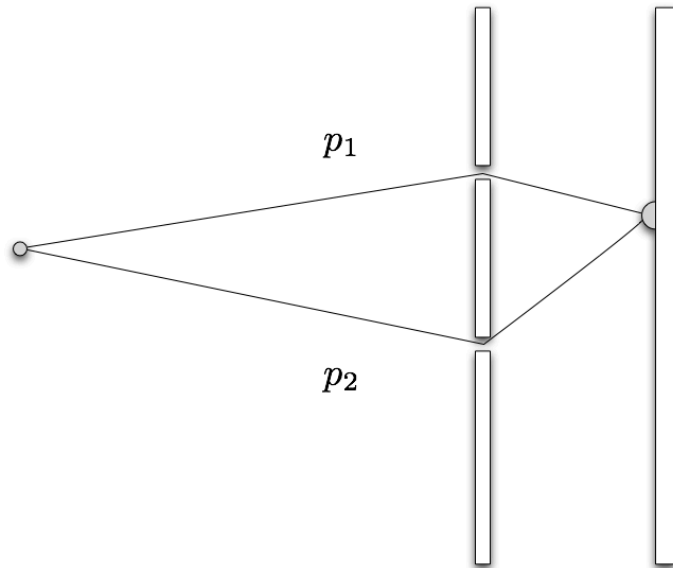


Additivity axiom

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.

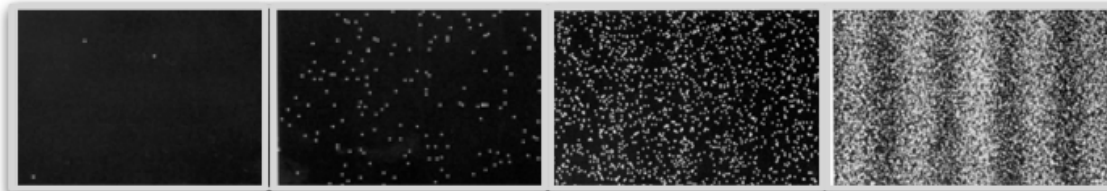


Nature ignores additivity axiom



THIS IS WHAT YOU EXPECT

THIS IS WHAT YOU OBSERVE



HITACHI DOUBLE SLIT EXPERIMENT WITH INDIVIDUAL ELECTRONS

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, & igitur residui, si aliquid
maneret, addita & detracta ex a c, ostende-
ret partes, at quia tale residuum est minus,
ideo imaginaberis & m̄. 15. id est differen-
tiæ a d, & quadrupli a b, quam adde &
minue ex a c, & habebis quæsitum, scili-
cet 5. p̄. & v. 25. m̄. 40. & 5. m̄. & v. 25.
m̄. 40. seu 5. p̄. & m̄. 15. & 5. m. & m.
15. duc 5. p̄. & m. 15. in 5. m. & m. 15.
dimissis incruciationibus, fit 25. m. m. 15.
quod est p̄. 15. igitur hoc productum est
40. natura tamen a d, non est eadem cum
natura 40. nec a b, quia superficies est

5. p̄. & m̄. 15.

5. m̄. & m. 15.

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

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

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

$$25 - (-15)$$

$$25 + 15$$

$$40$$

Complex numbers



$$\alpha = a + i b$$

$$i = \sqrt{-1}$$

$$i^2 = -1$$

Modern notation

Karl Friedrich Gauss

1777-1855

$$3 + i42 \quad \sqrt{6} \quad \sqrt{-6} = i\sqrt{6}$$



purely real



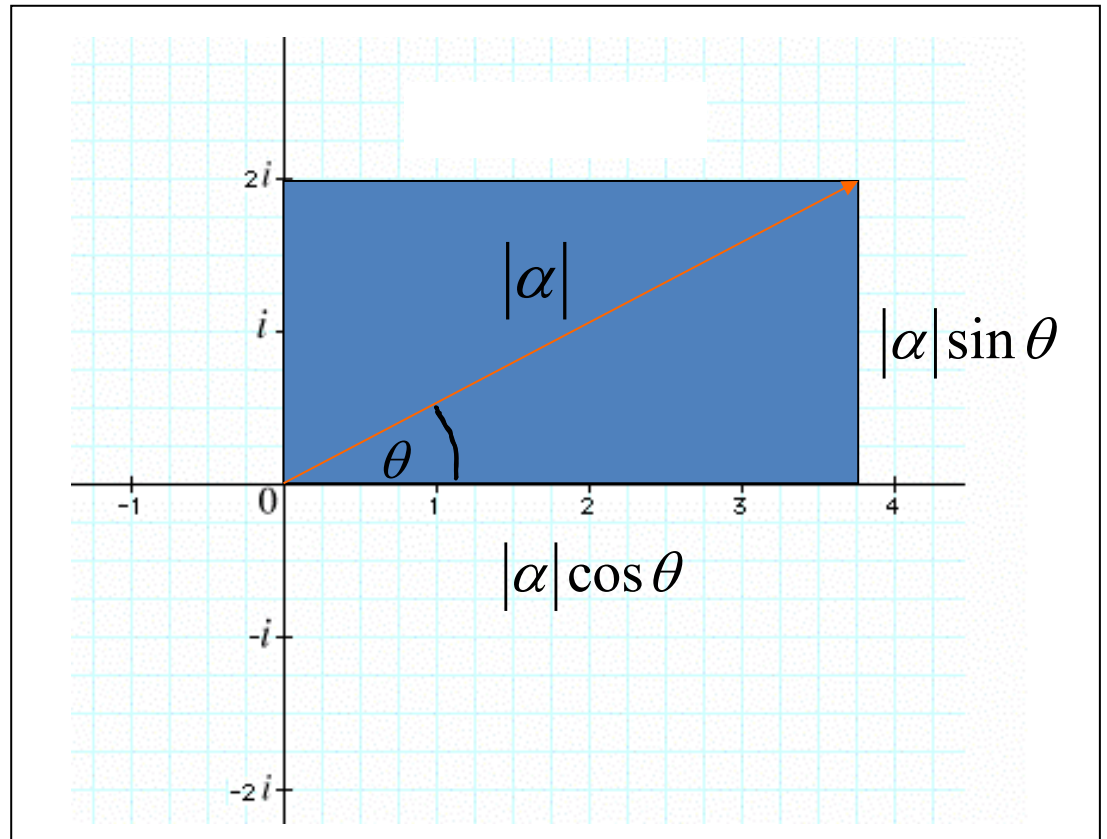
purely imaginary

Geometric representation



Leonhard Euler
1707-1783

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



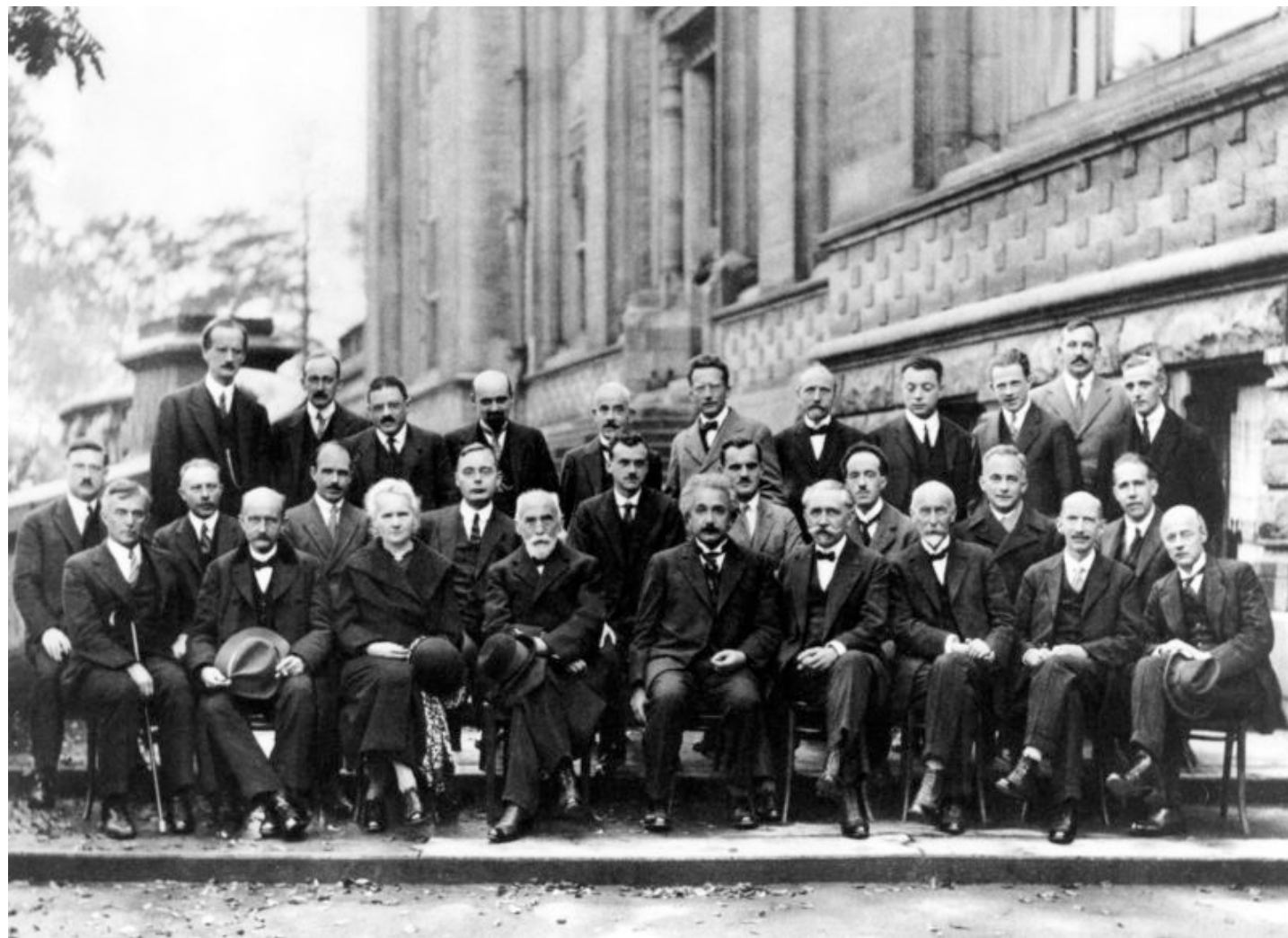
Do you understand complex numbers?

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?

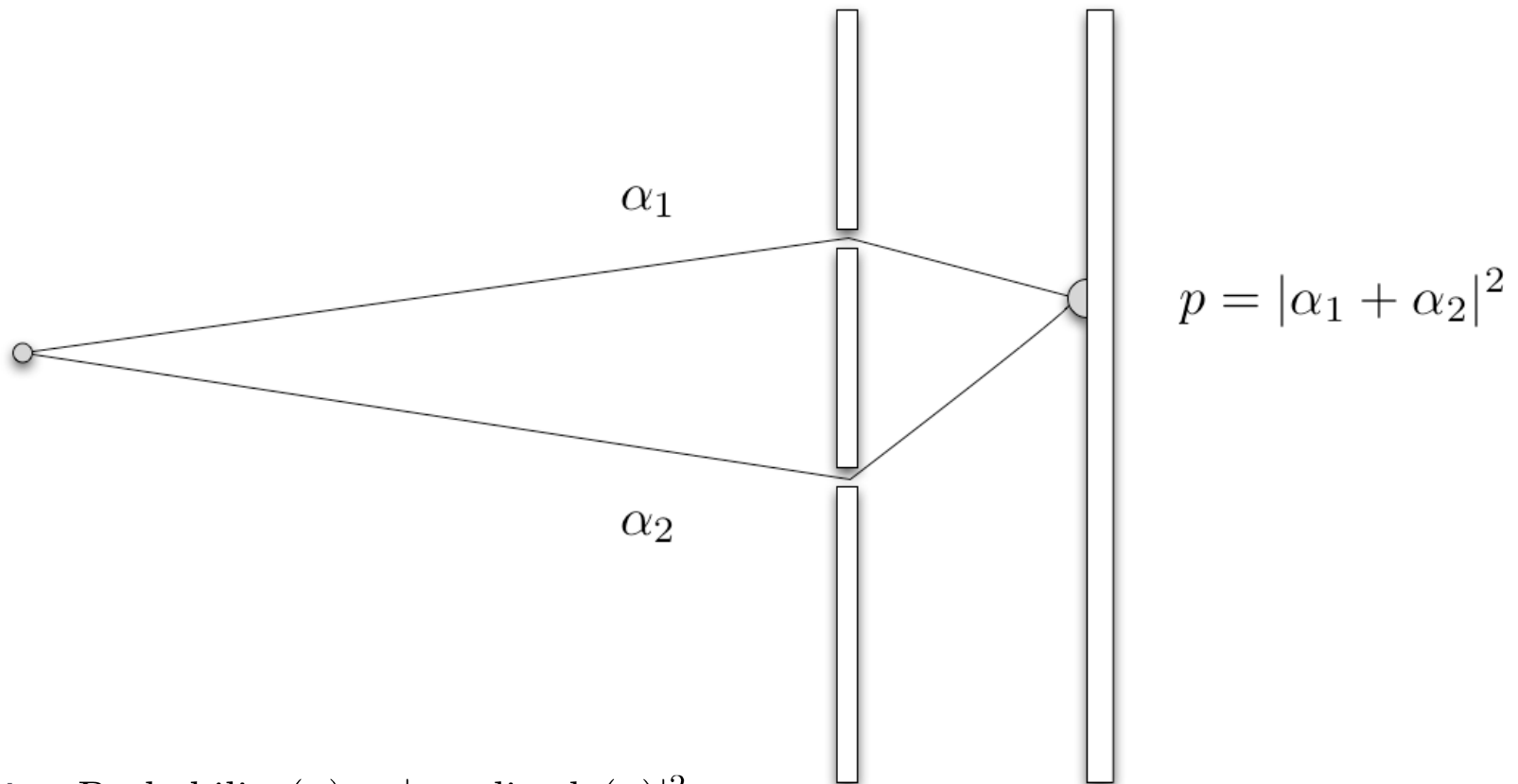
Enter quantum theory



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

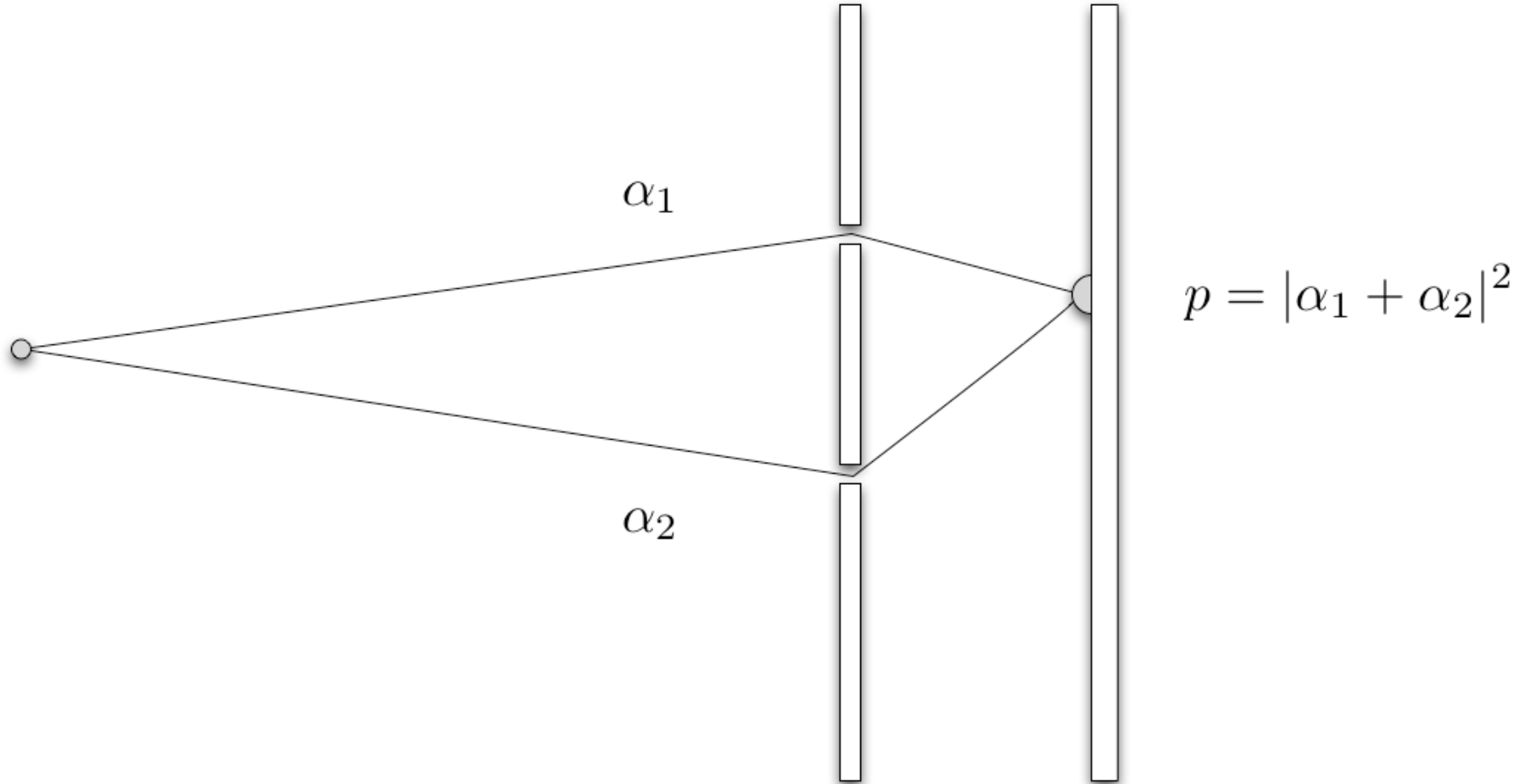
1926

[†] 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.].

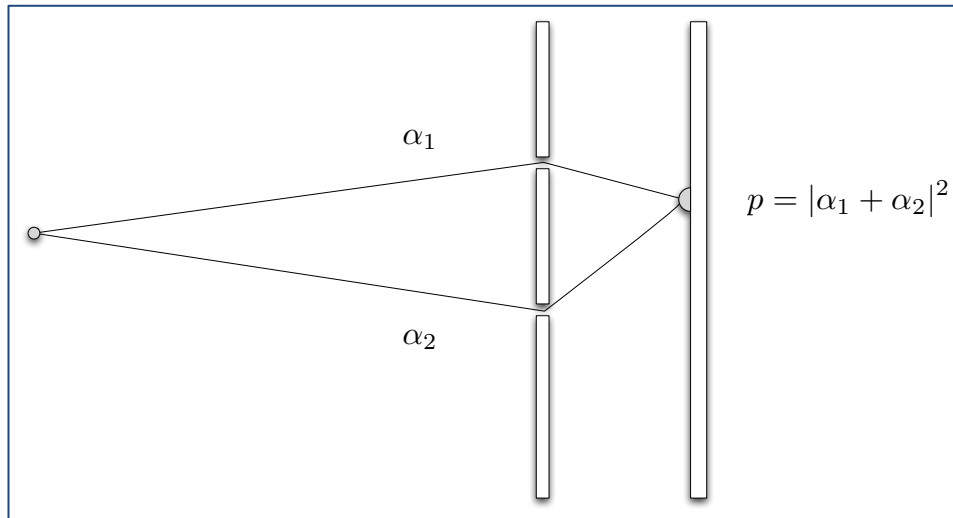
If one translates this result into terms of particles, only one interpretation is possible. $\Phi_{n,\tau,m}(\alpha, \beta, \gamma)$ gives the probability* for the electron, arriving from the z -direction, to be thrown out into the direction designated by the angles α, β, γ , with the phase change δ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

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

Add amplitudes not probabilities



Quantum interference



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

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

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

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

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

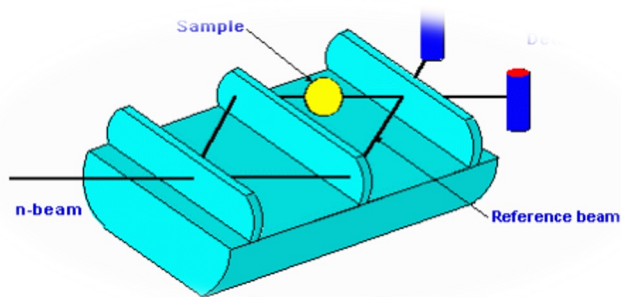
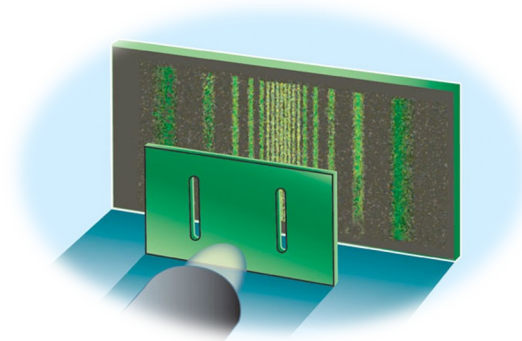
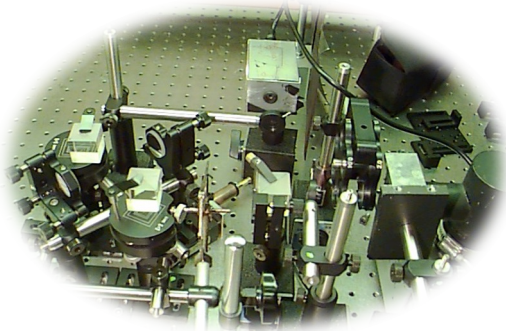
Quantum world is somewhat different...



©Charles Addams

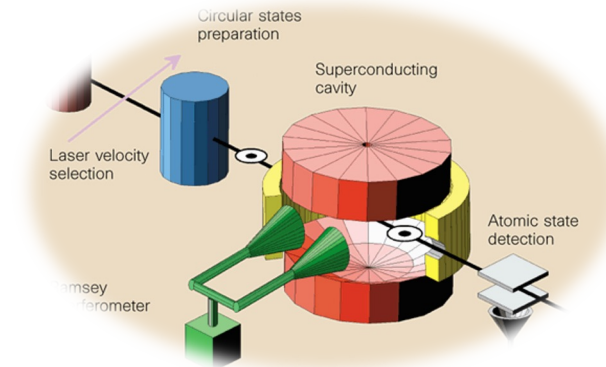
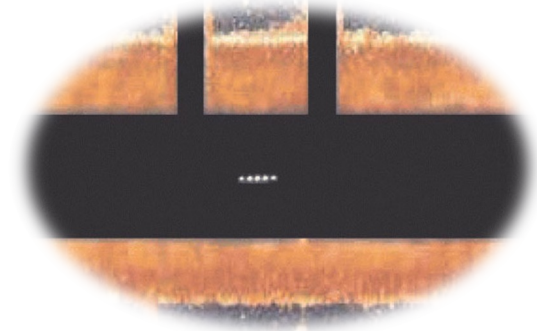
Ubiquitous quantum interference

PHOTONS



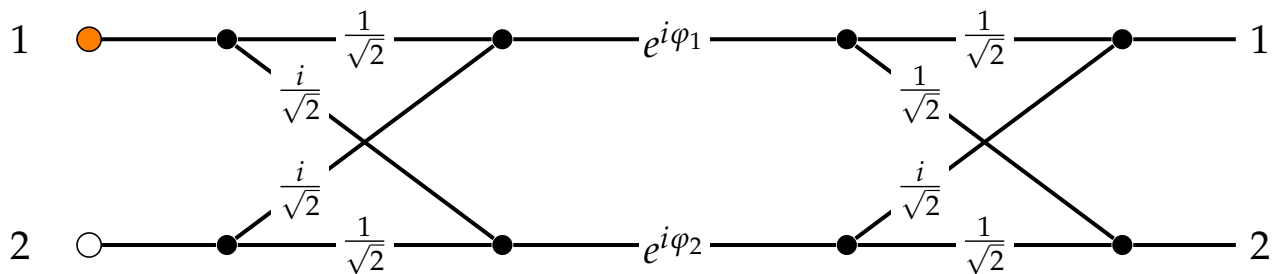
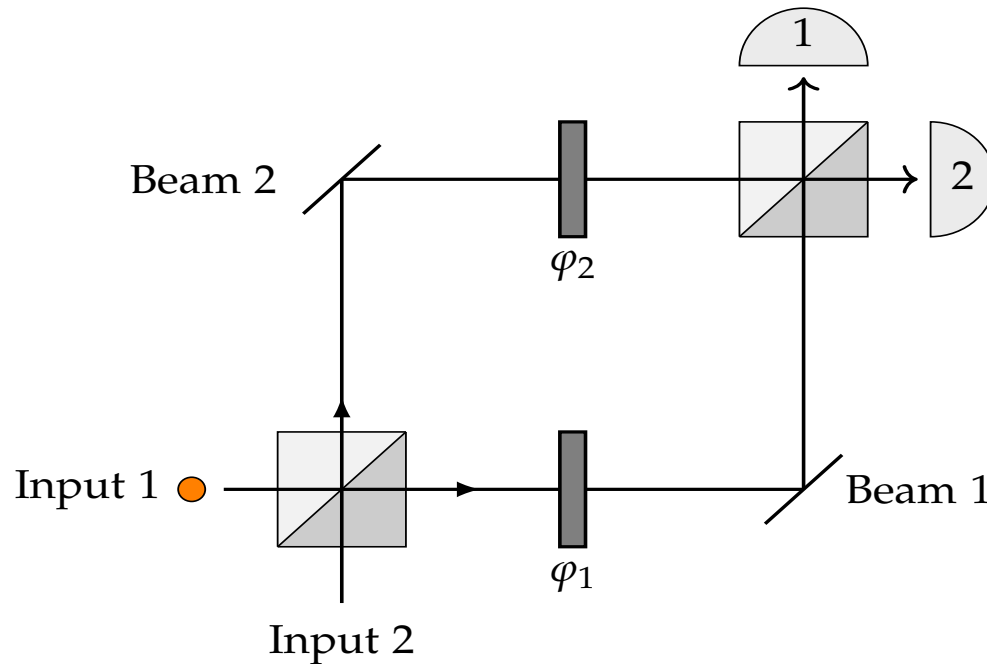
NEUTRONS

IONS



ATOMS

Mach-Zehnder interferometer

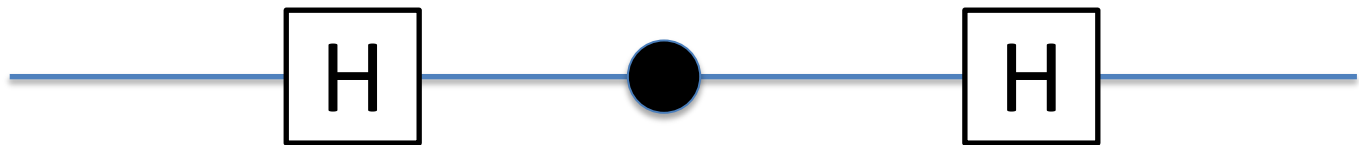
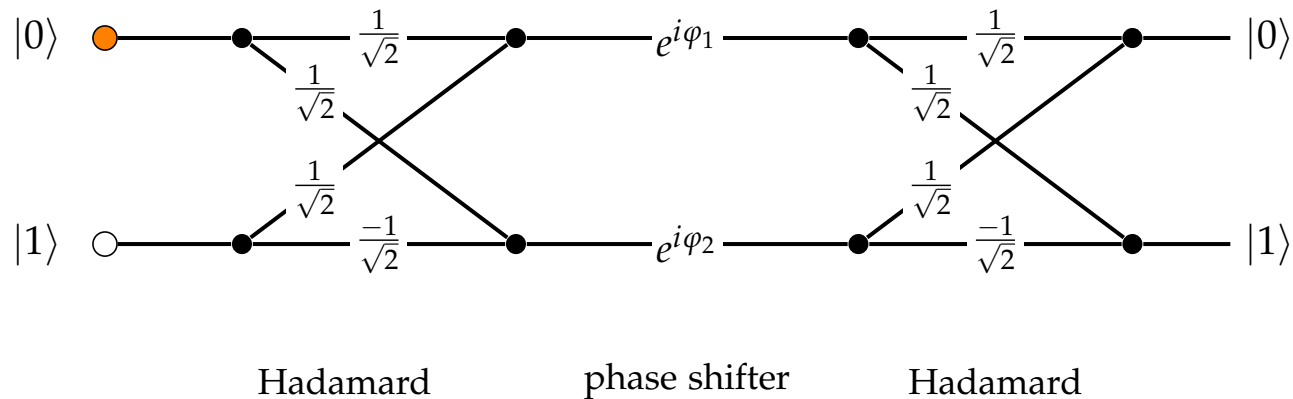


first beamsplitter

phase shifts

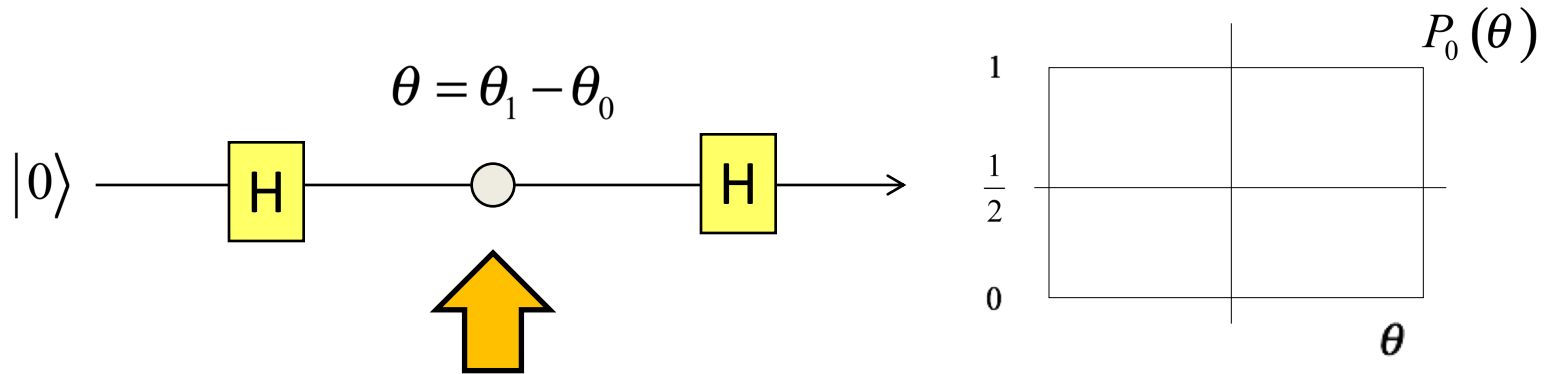
second beamsplitter

In terms of gates and circuits...



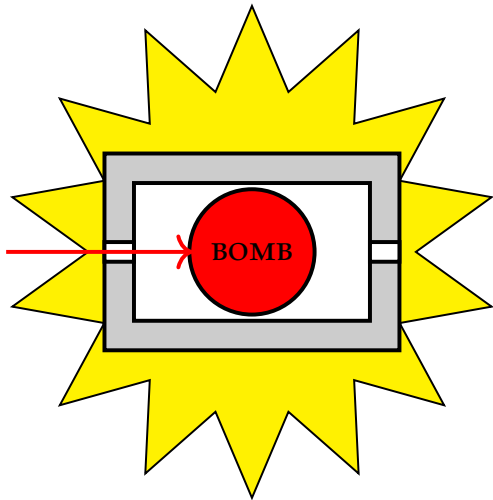
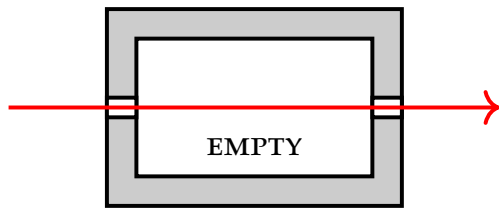
$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix}
 \begin{bmatrix} e^{i\varphi_0} & 0 \\ 0 & e^{i\varphi_1} \end{bmatrix}
 \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix}$$

Quantum gravimeters, acelerometers

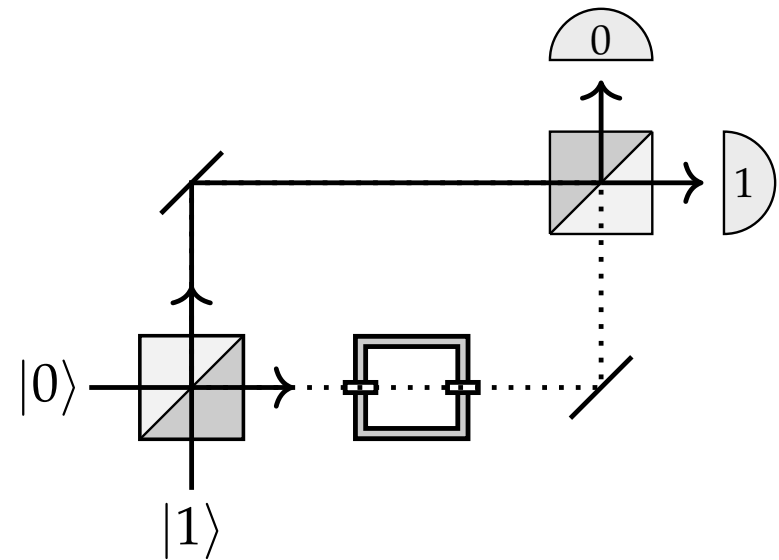


- Accelerations
- Rotations
- Laser frequency detuning
- Laser phase
- Photon recoil
- Electric/magnetic fields
- Interactions with atoms and molecules

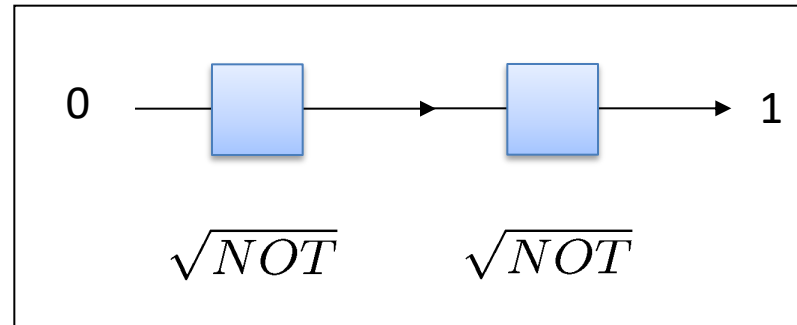
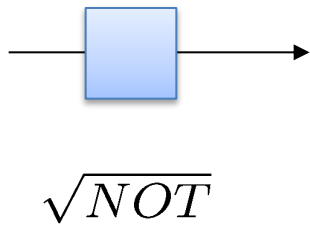
Can you detect super-sensitive bombs?



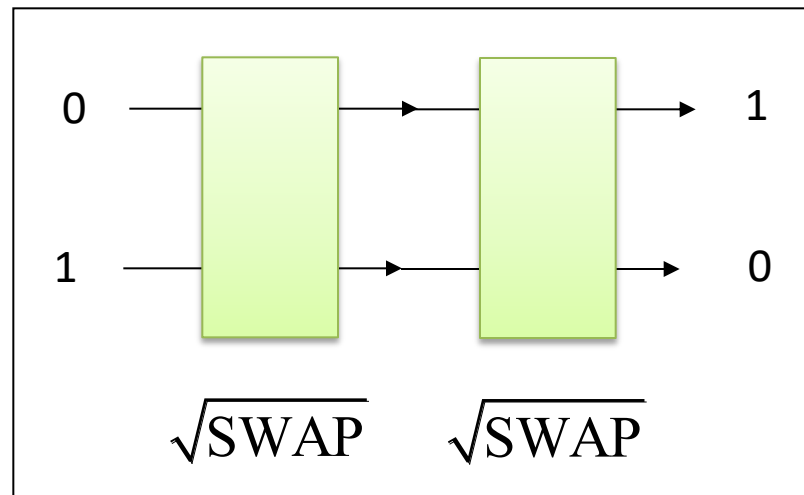
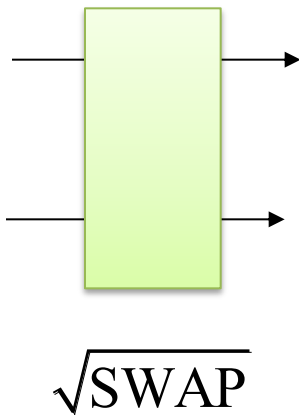
Hint: Consider the setup where the input and output ports are hooked up in one of the arms of a Mach-Zehnder interferometer.



Logically impossible gates

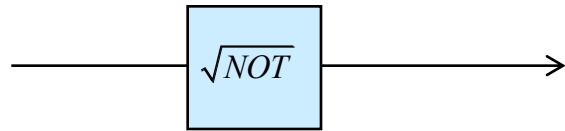


NOT



SWAP

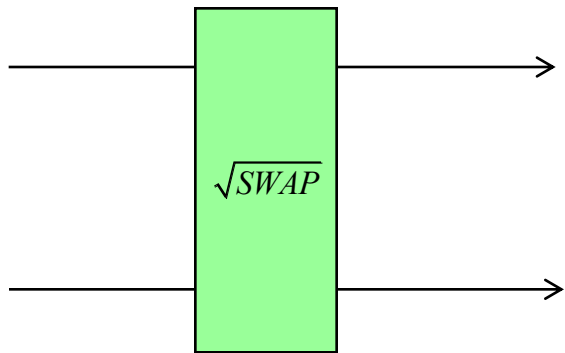
This is all we need...



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

Generates superpositions

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



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

Generates entanglement

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



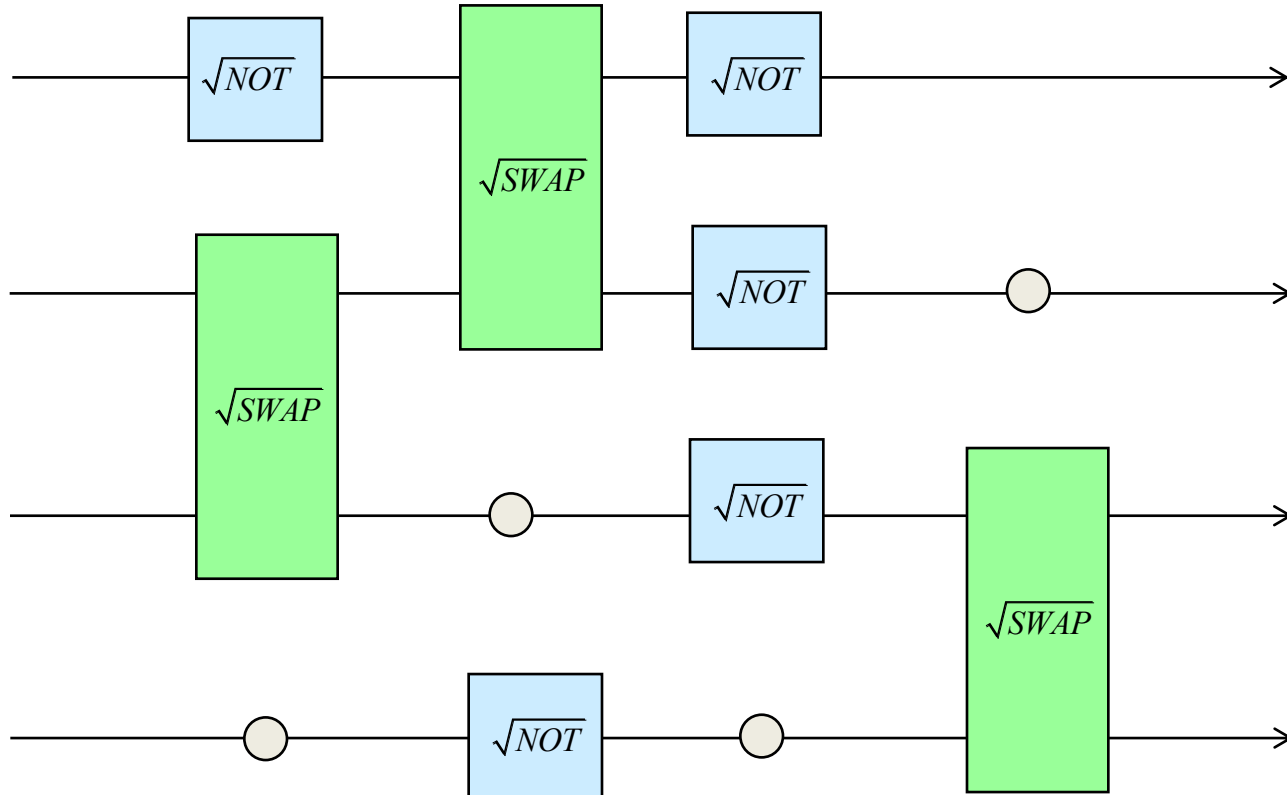
$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$$

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

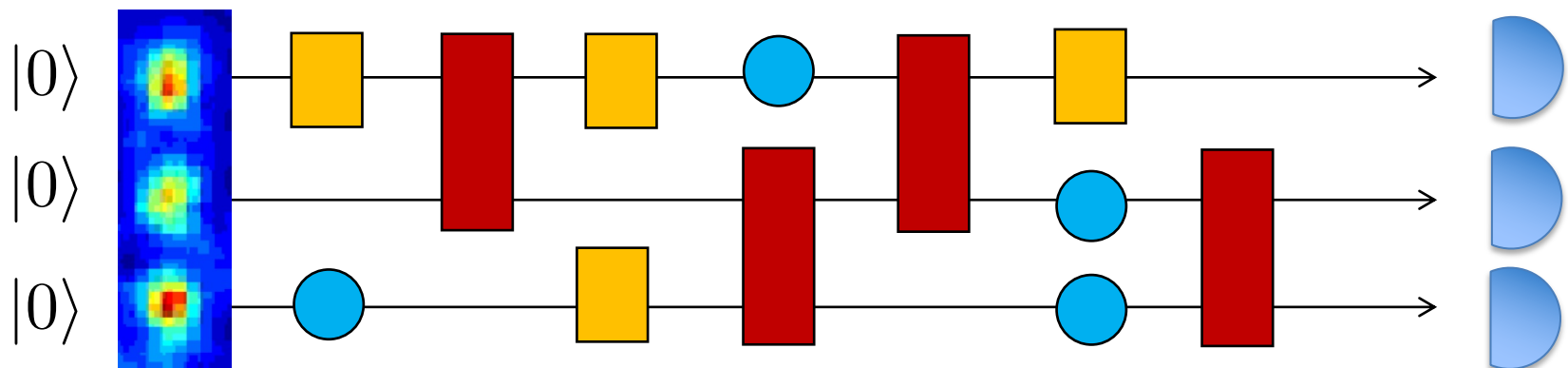
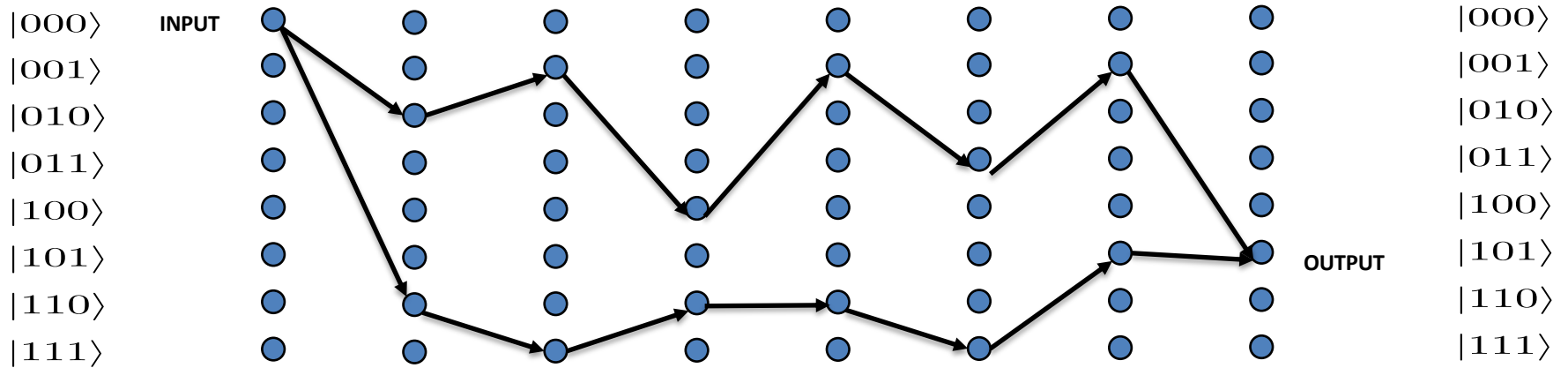
$$|0\rangle \rightarrow |0\rangle \quad |1\rangle \rightarrow e^{i\varphi} |1\rangle$$

Quantum circuits with impossible gates

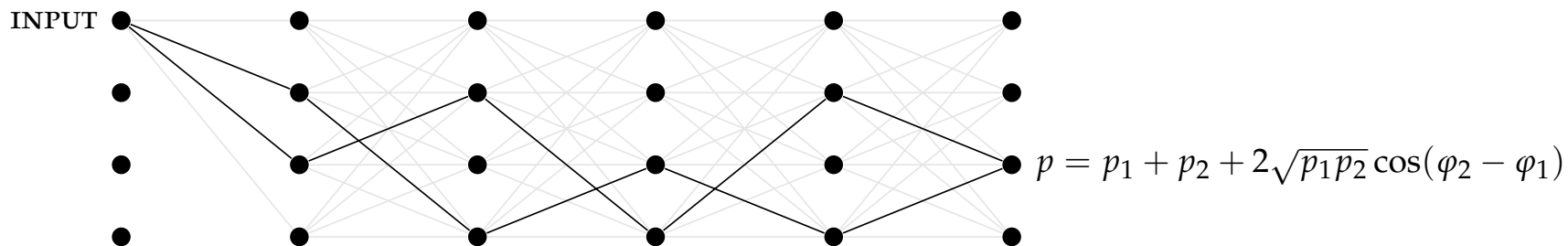
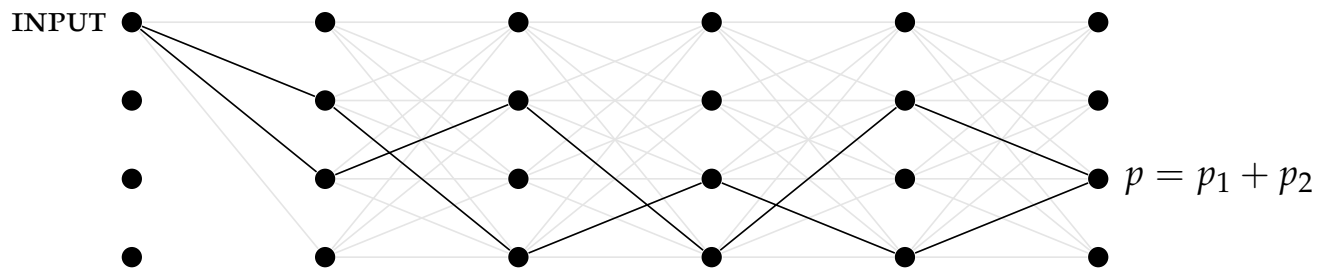
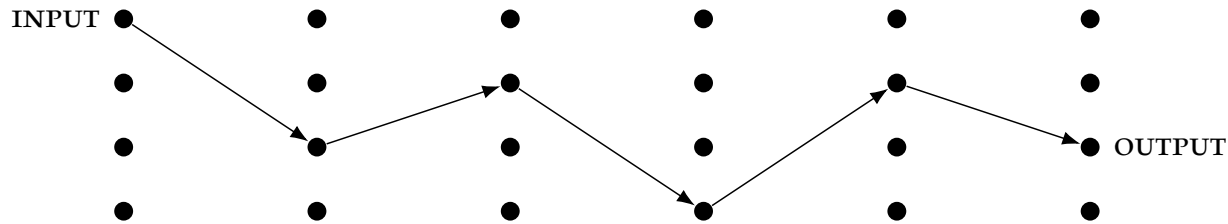
QUANTUM BITS = QUBITS



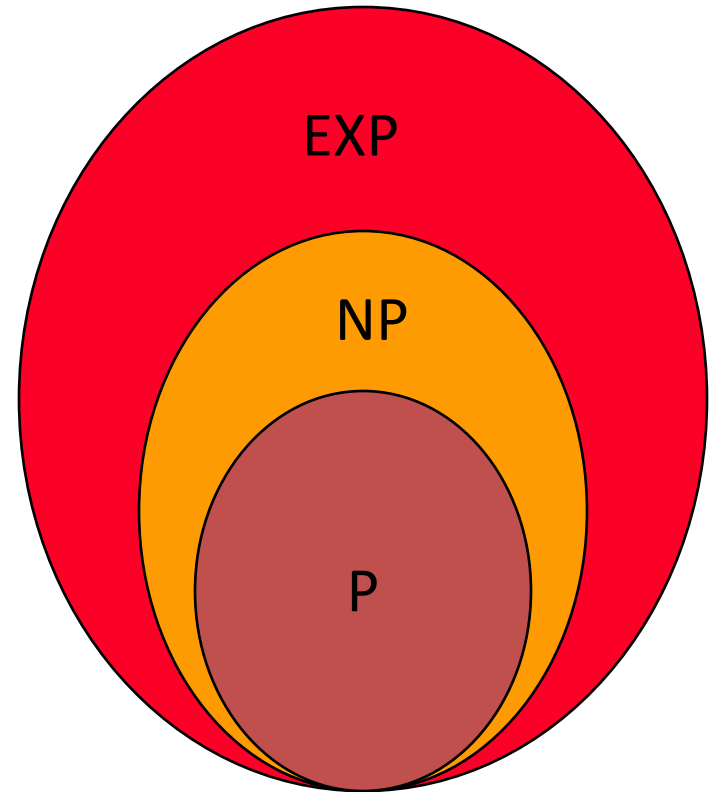
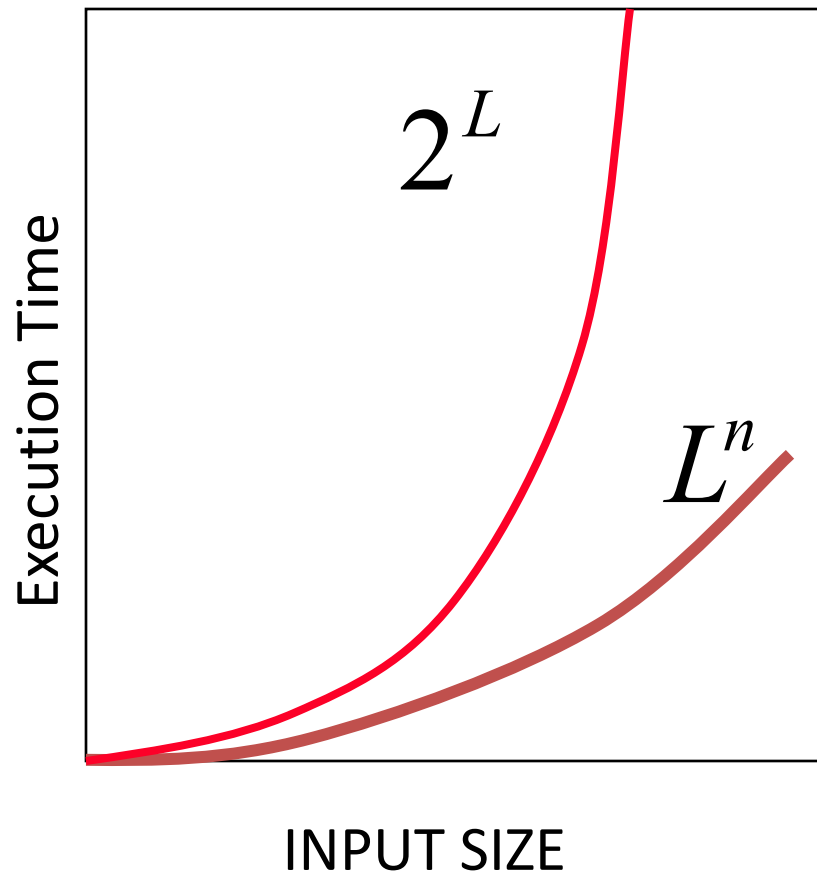
Multi-particle interference (quantum computation)



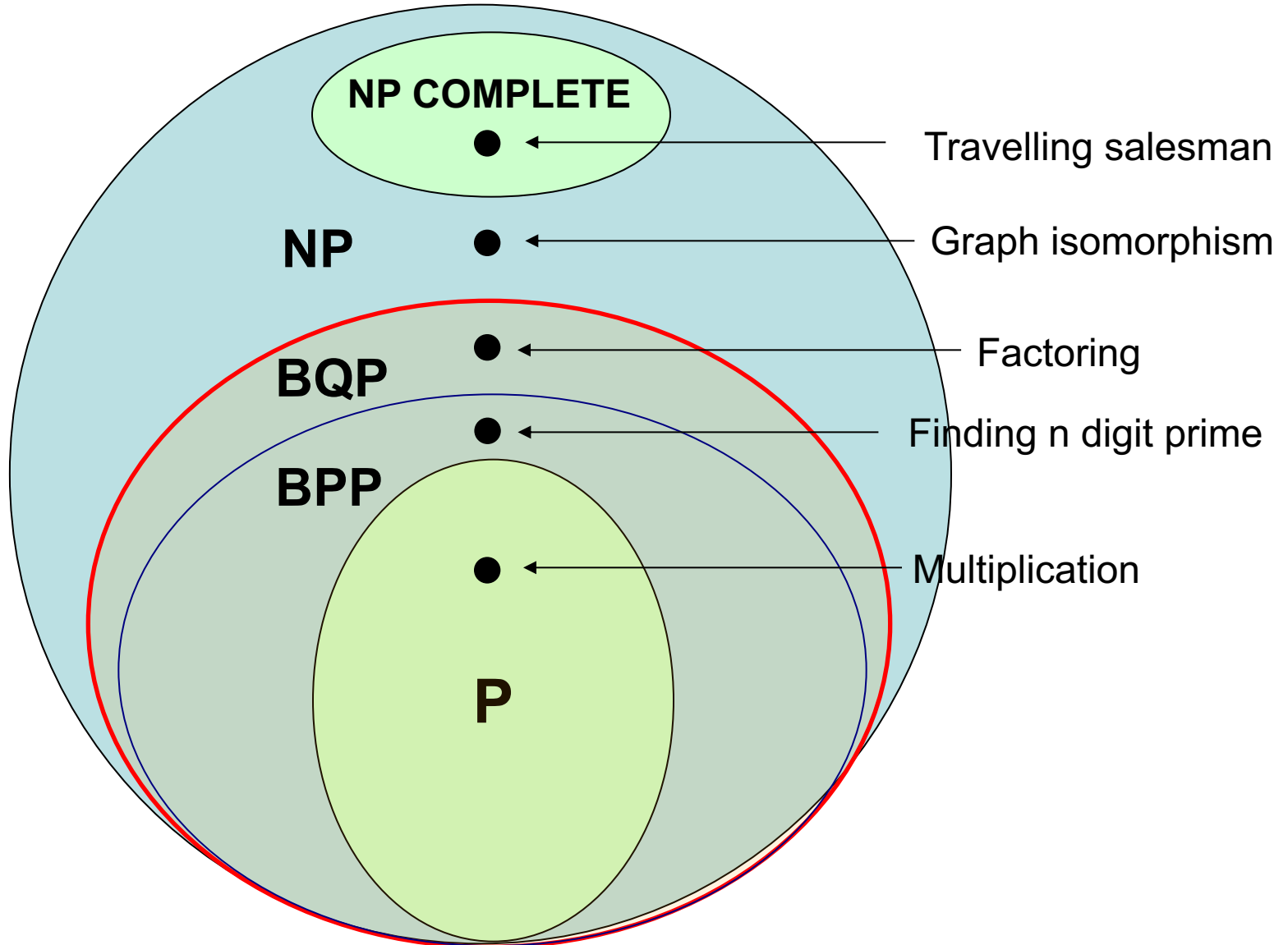
Deterministic, probabilistic and quantum



Hard and easy...



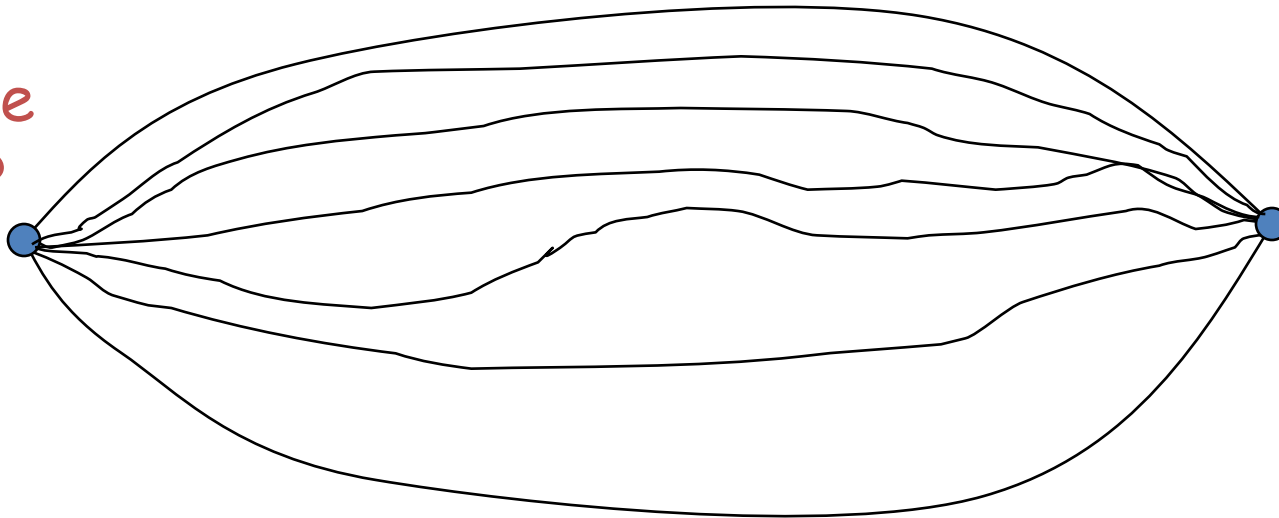
Zoo of computational complexity



Impact on logic...

Traditional approach: proof = physical record

Is A true
or not ?

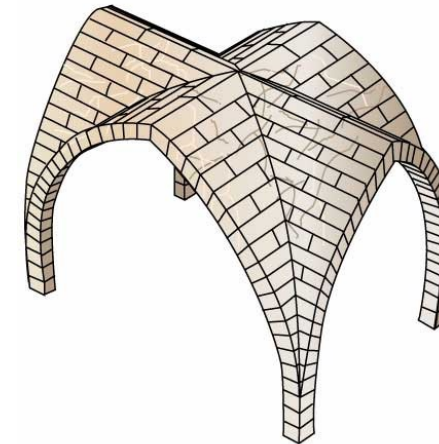
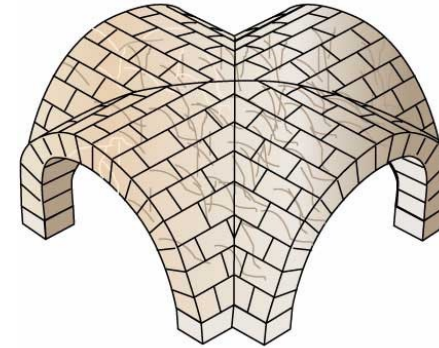
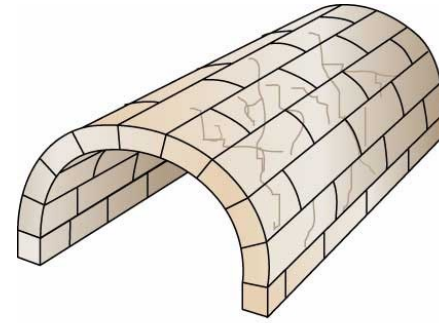


Yes, A
is true!

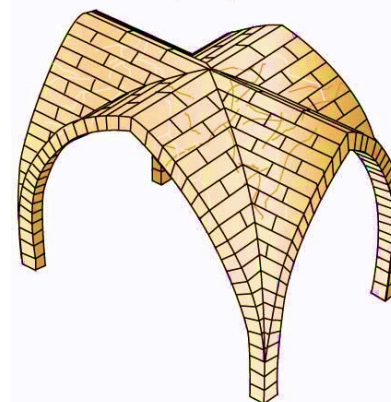
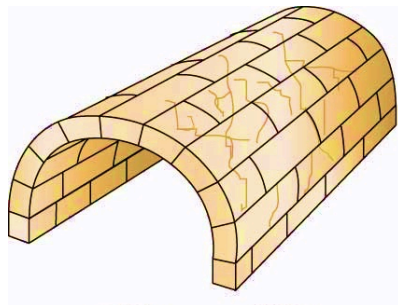
Testing 10^{100} different possibilities in quantum superpositions

Proof = physical process

Limits to quantum computation ?



Building quantum computers...

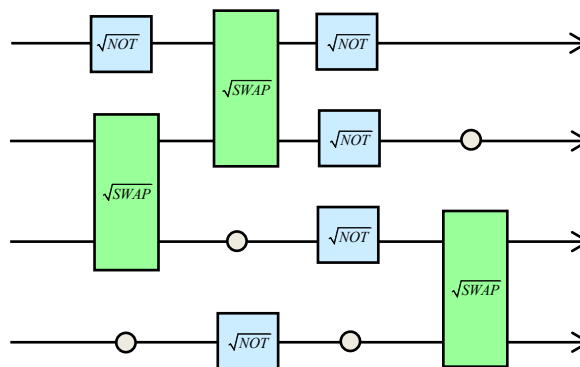
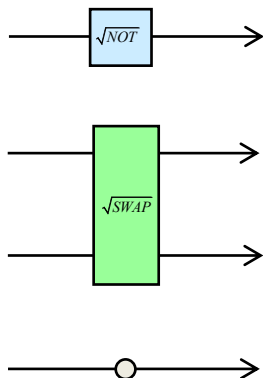


Basic blocks

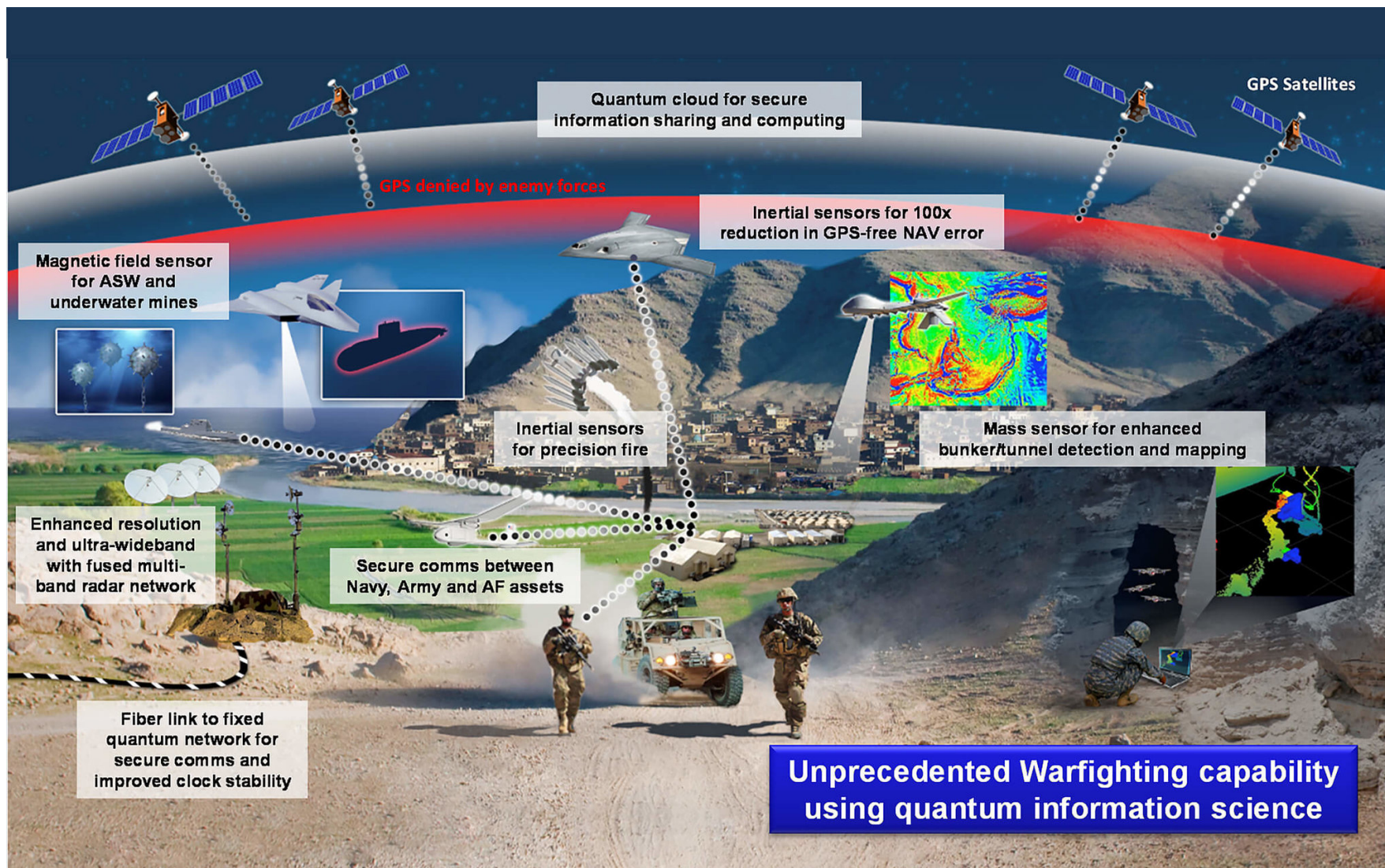
Stable & fault tolerant

Scaling up

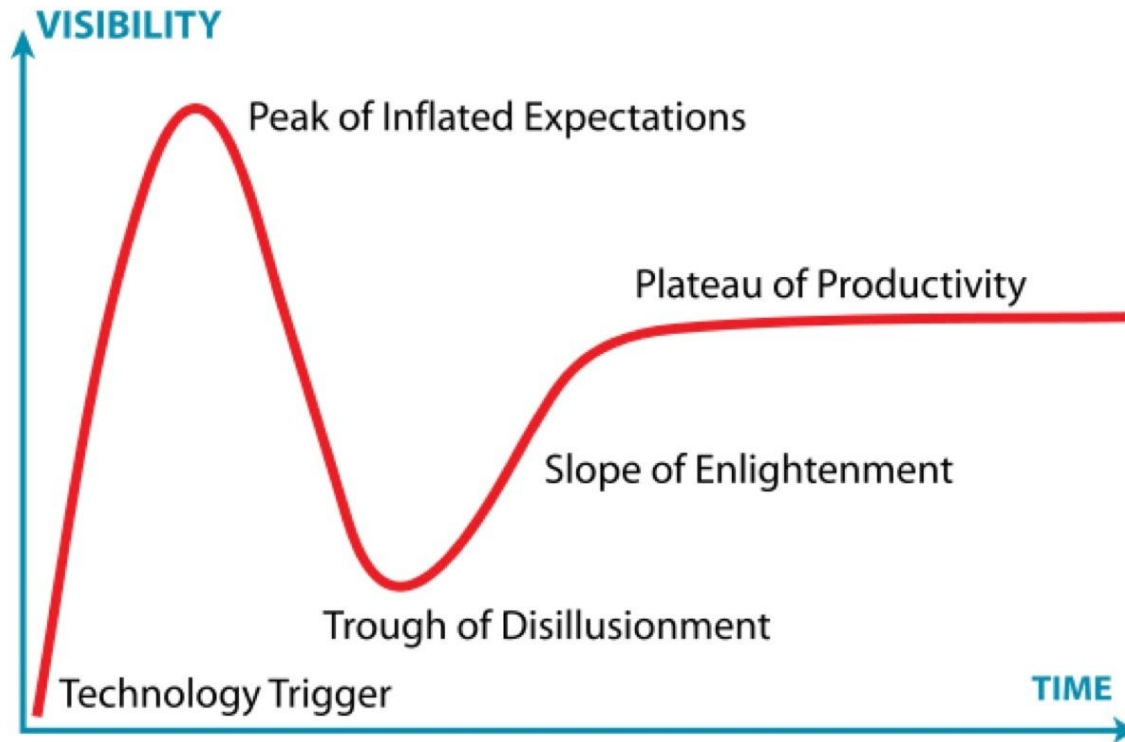
The final thing



Optimists – quantum advantage



Pessimists - the Gartner Hype Cycle

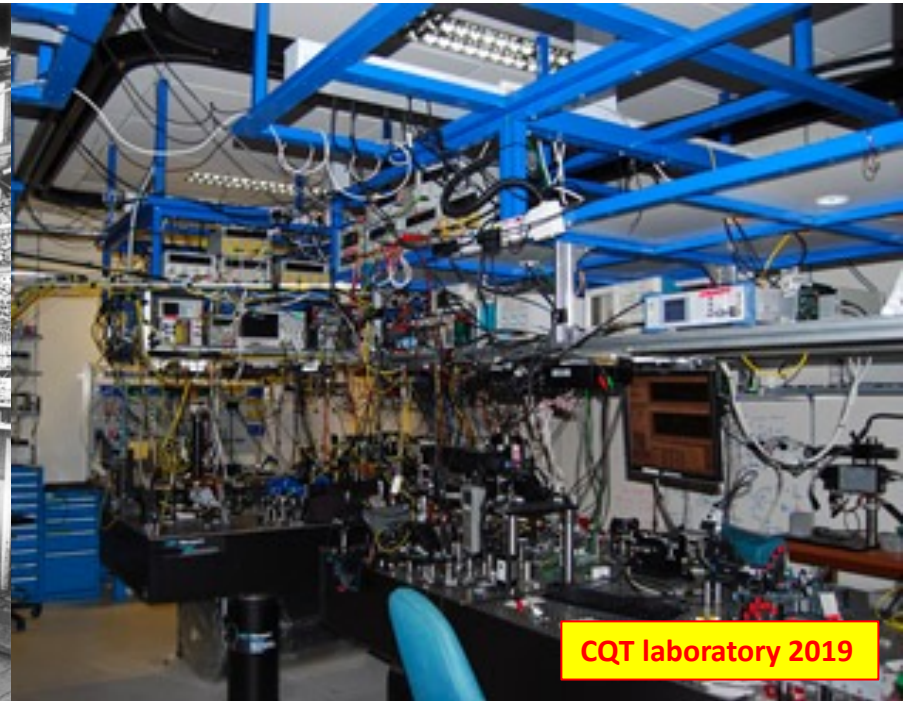


Humans are famously bad at predicting the future of technologies.

Computers & Physics

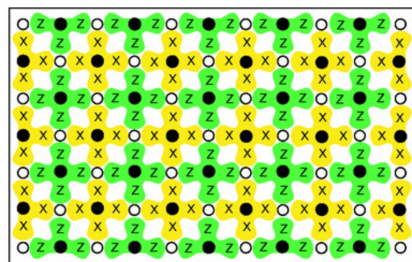
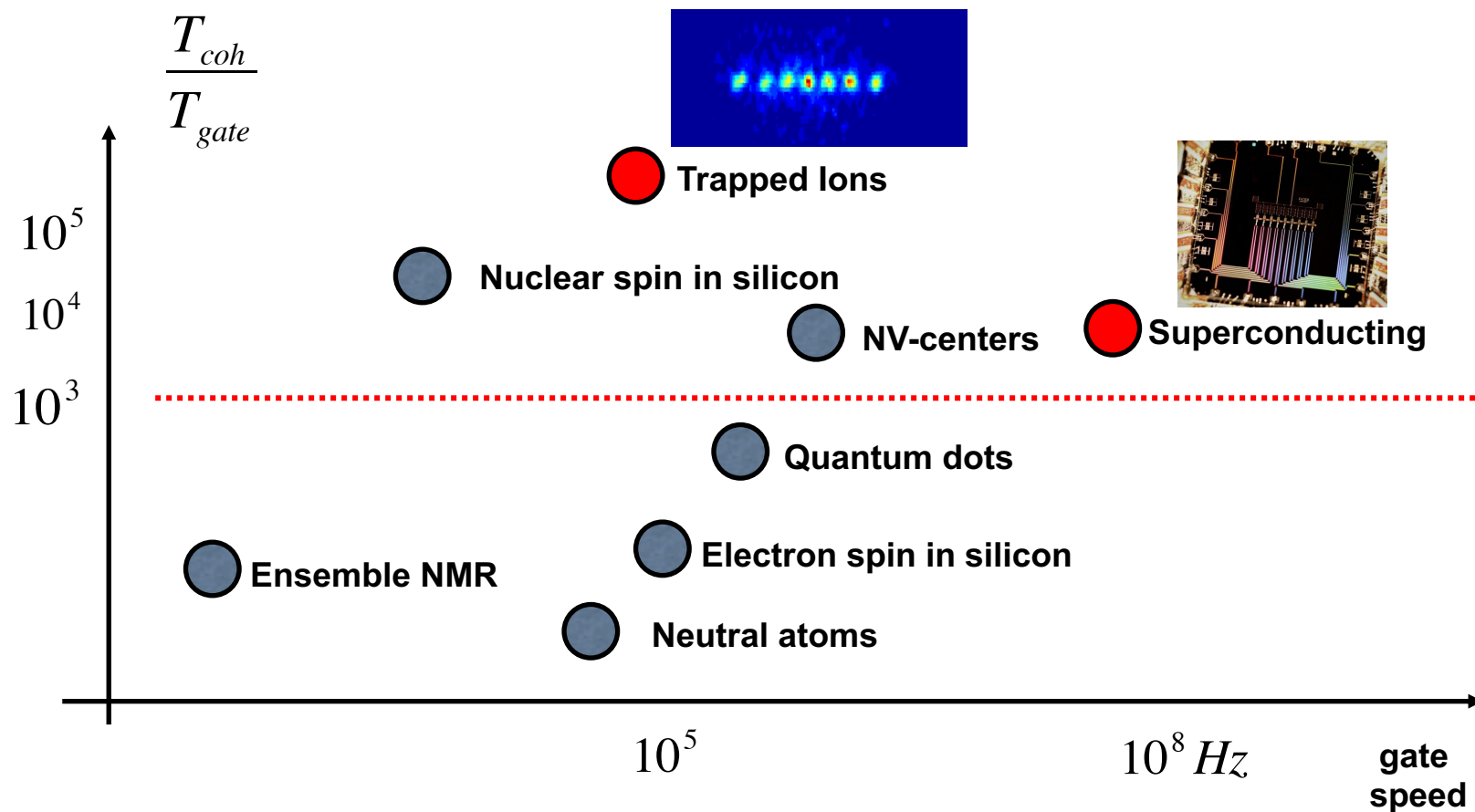


early classical computers



early quantum computers

Practicalities...



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

When, when, when... ?

Individual expert opinions of likelihood of a quantum computer able to break RSA-2048 in 24 hours

(respondents close to experiment)

Extremely likely
(> 99% chance)

Very likely
(> 95% chance)

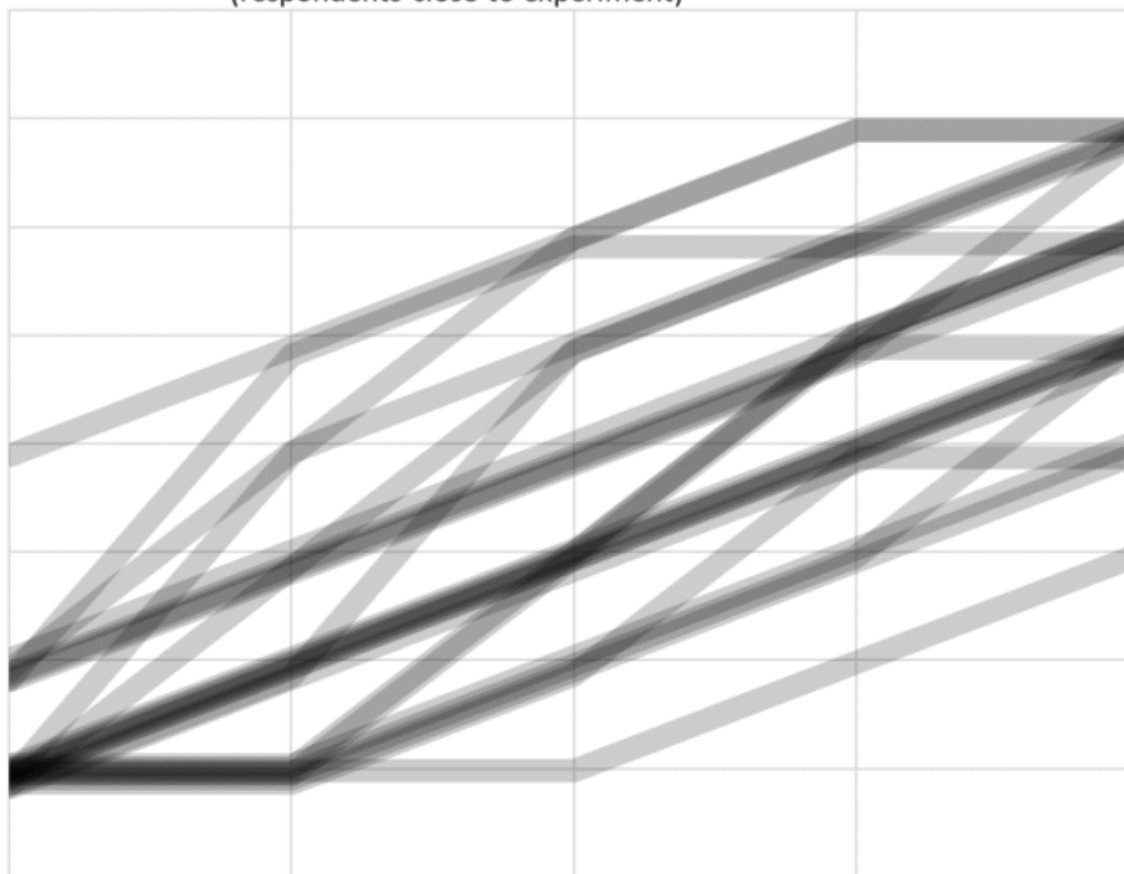
Likely
(> 70% chance)

Neither likely not
unlikely
(~ 50% chance)

Unlikely
(< 30% chance)

Very unlikely
(< 5% chance)

Extremely unlikely
(< 1% chance)



within 5 years

within 10 years

within 15 years

within 20 years

within 30 years

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

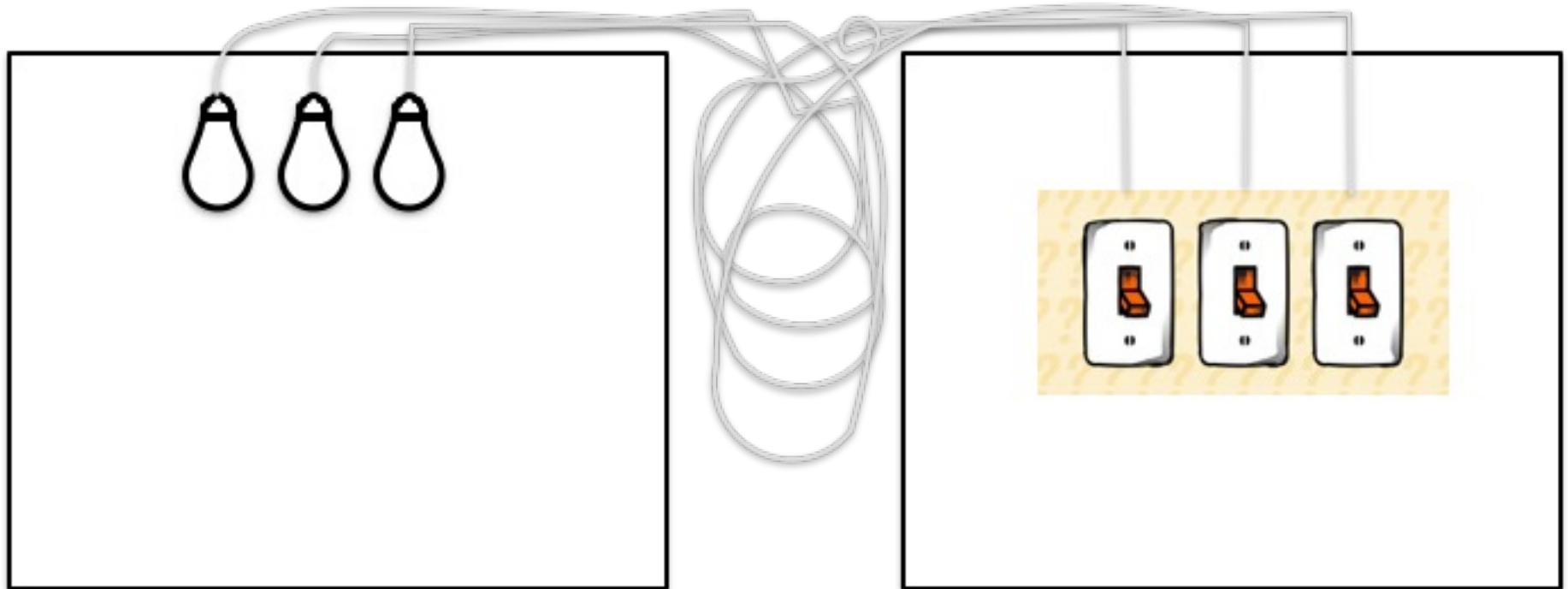
Quantum computing

New quantum algorithms for solving hard problems.

Quantum simulation

Probes of exotic quantum many-body phenomena.

Think like a physicist



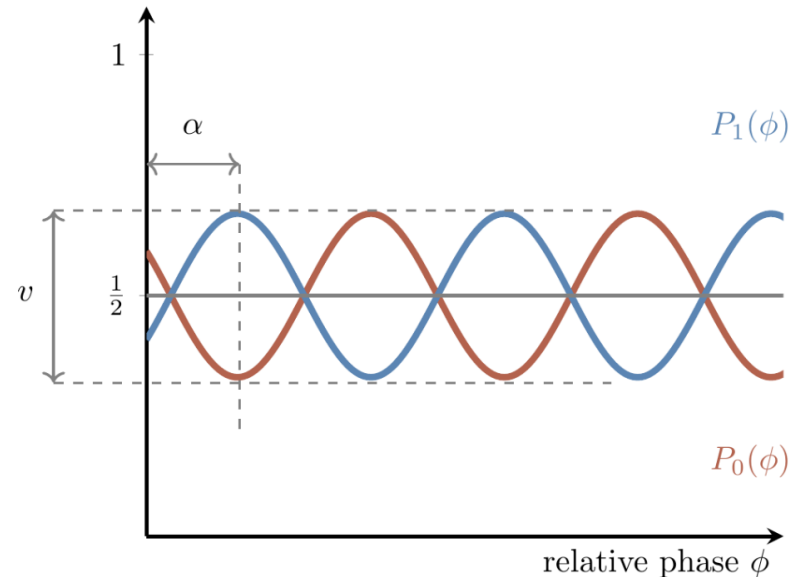
Decoherence

$$|0\rangle \xrightarrow{H} \bullet \xrightarrow{\varphi} \xrightarrow{H} \cos \frac{\varphi}{2} |0\rangle - i \sin \frac{\varphi}{2} |1\rangle$$

$$|0\rangle|e\rangle \mapsto |0\rangle|e_{00}\rangle$$

$$|1\rangle|e\rangle \mapsto |1\rangle|e_{11}\rangle$$

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



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

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

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