Basics of Quantum Complexity

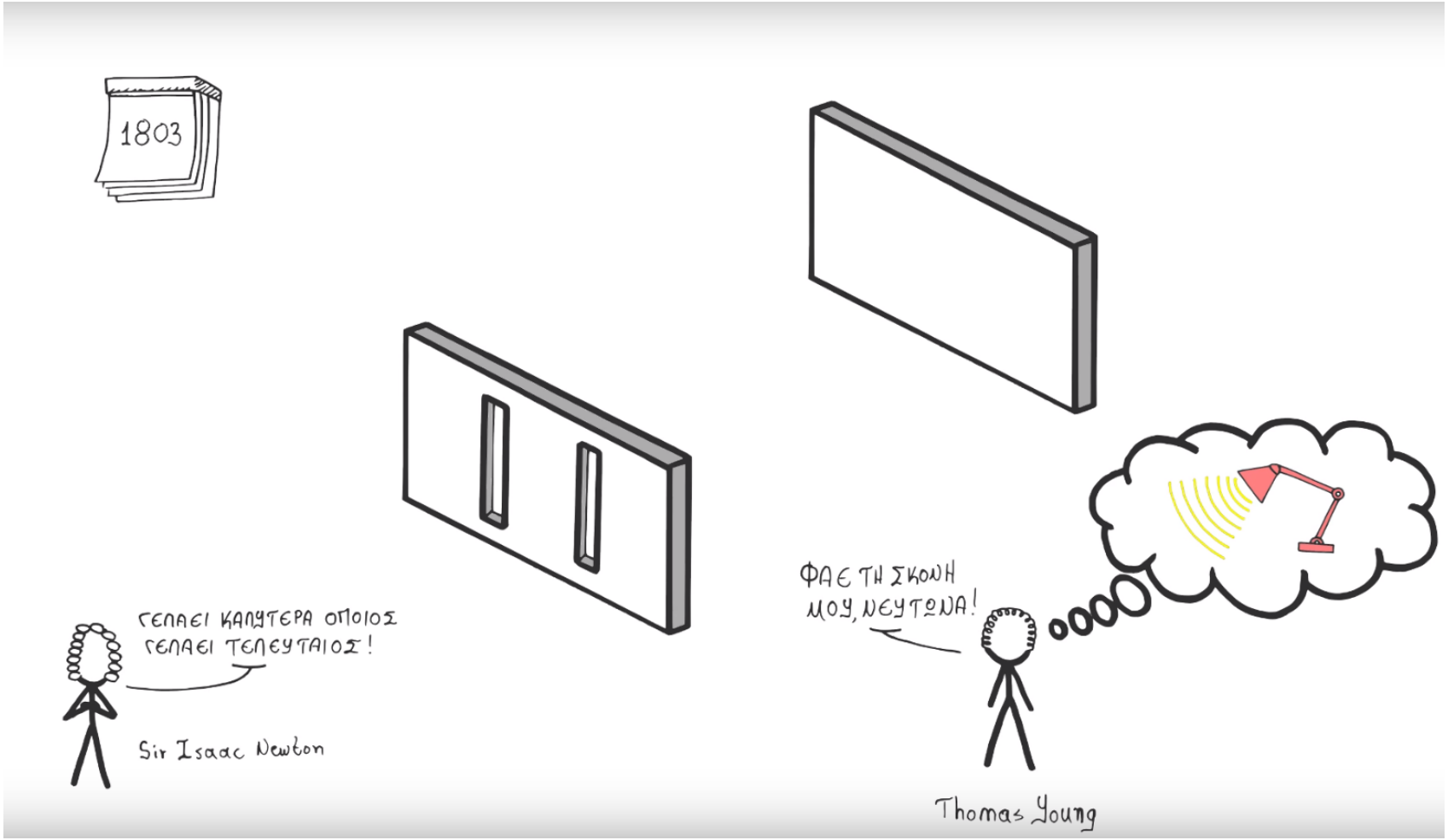
ECE, NTUA

June 1, 2018

Outline

The Double Slit Experiment

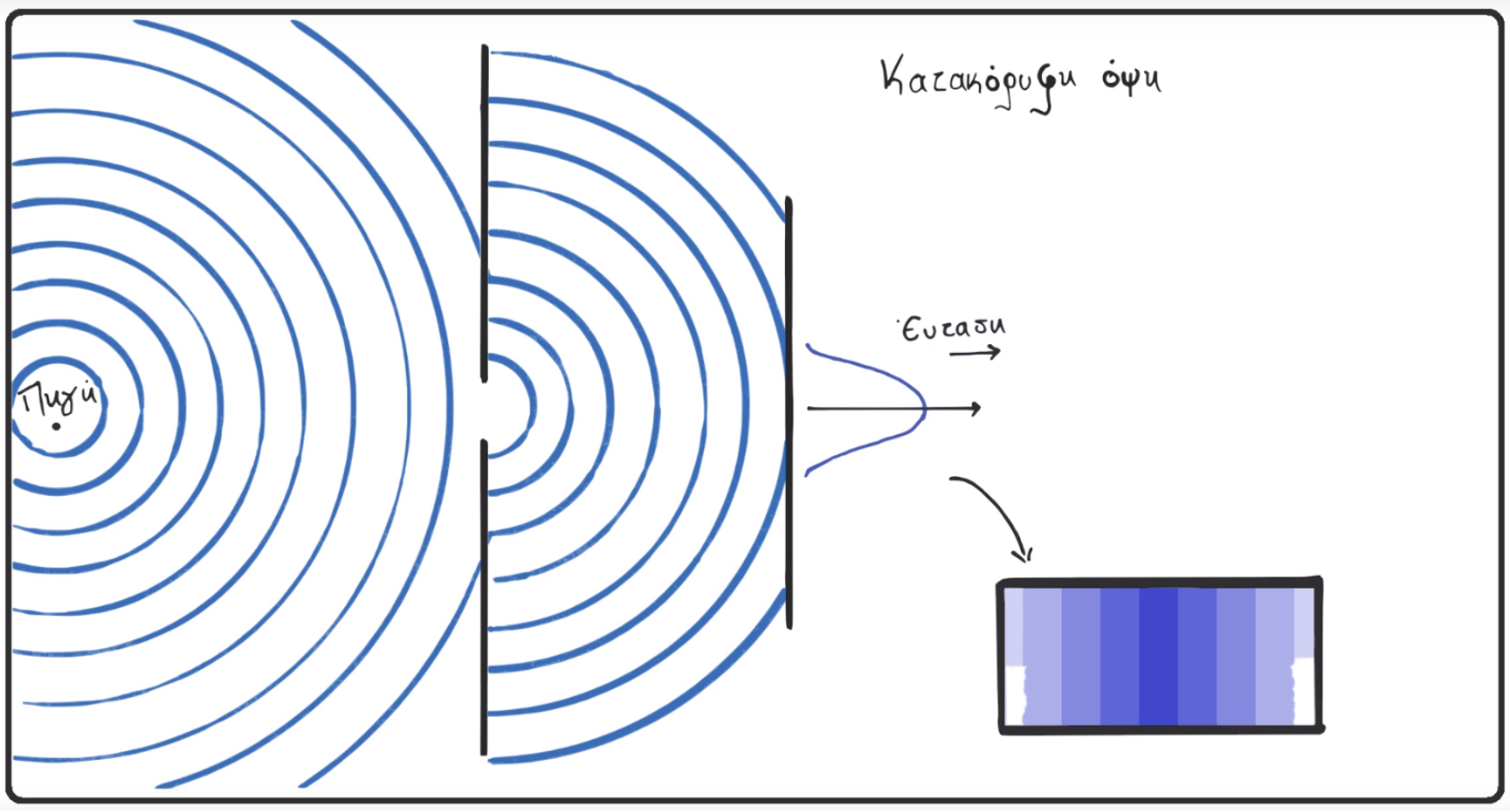
Light: Wave or particle?[1]



[1] *Images*: *Καθημερινη Φυσικη*

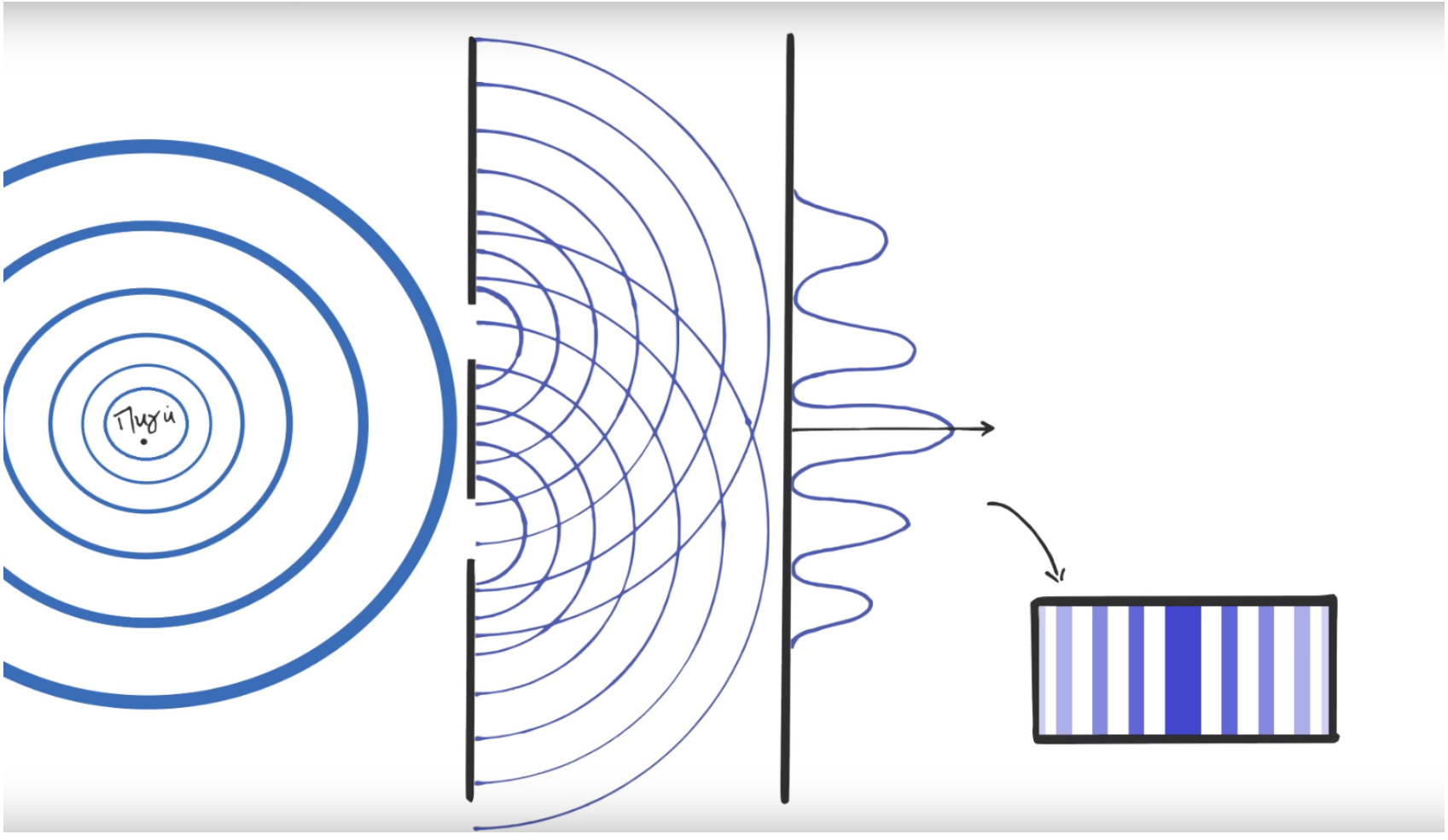
The Double Slit Experiment

Wave: Expected result (one slit)



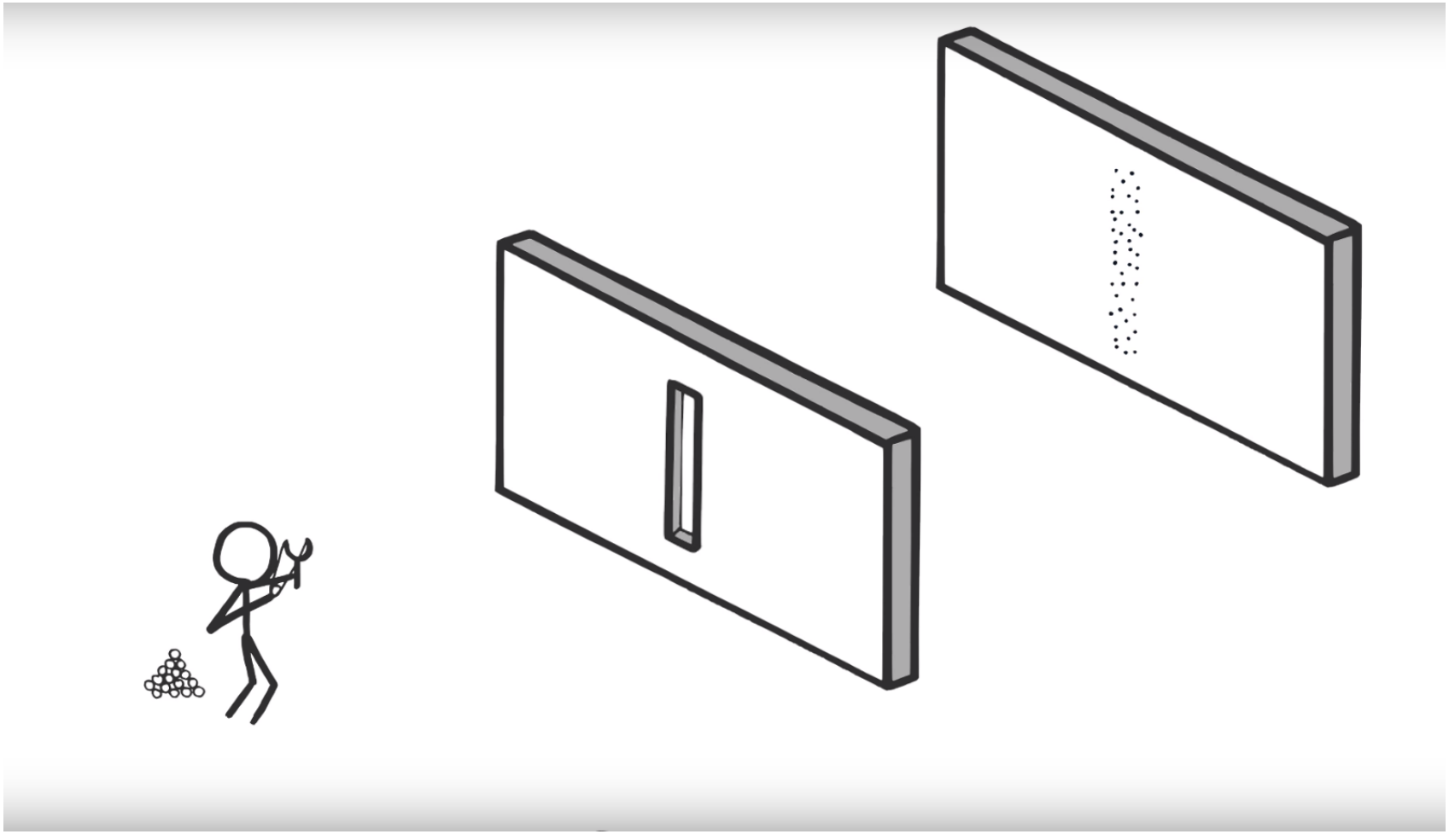
The Double Slit Experiment

Wave: Expected result (double slit)



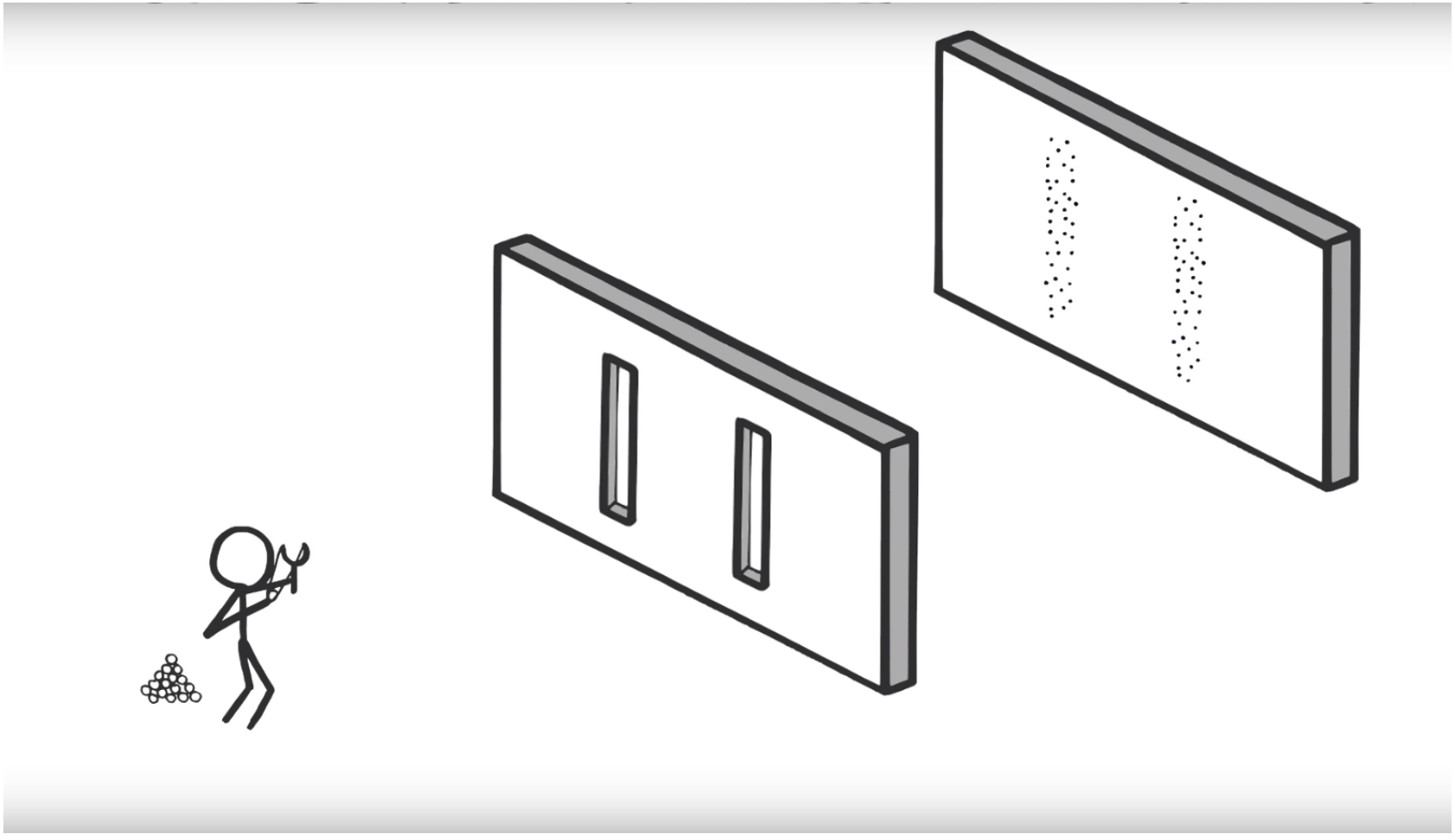
The Double Slit Experiment

Particle: Expected result (one slit)



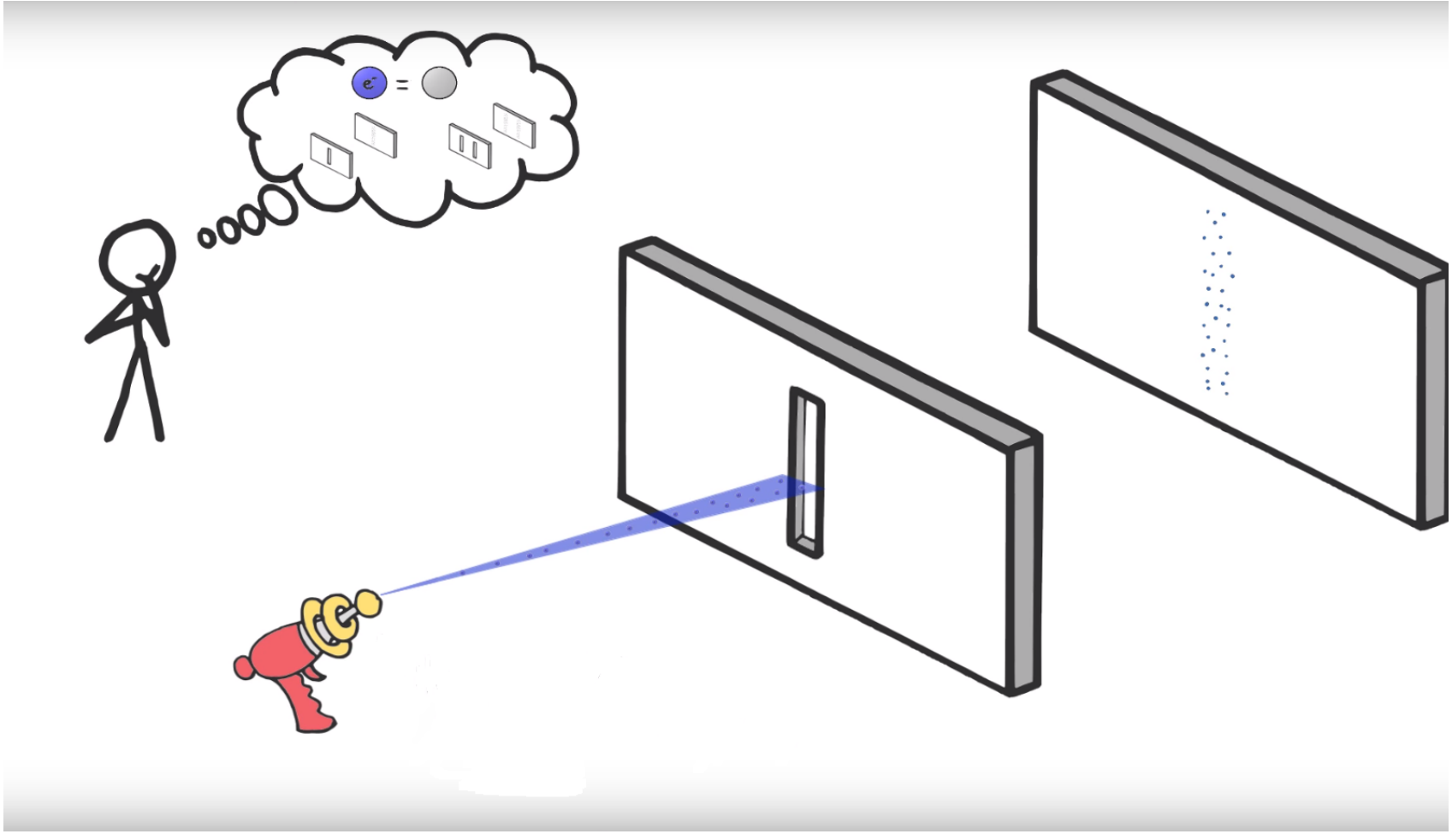
The Double Slit Experiment

Particle: Expected result (double slit)



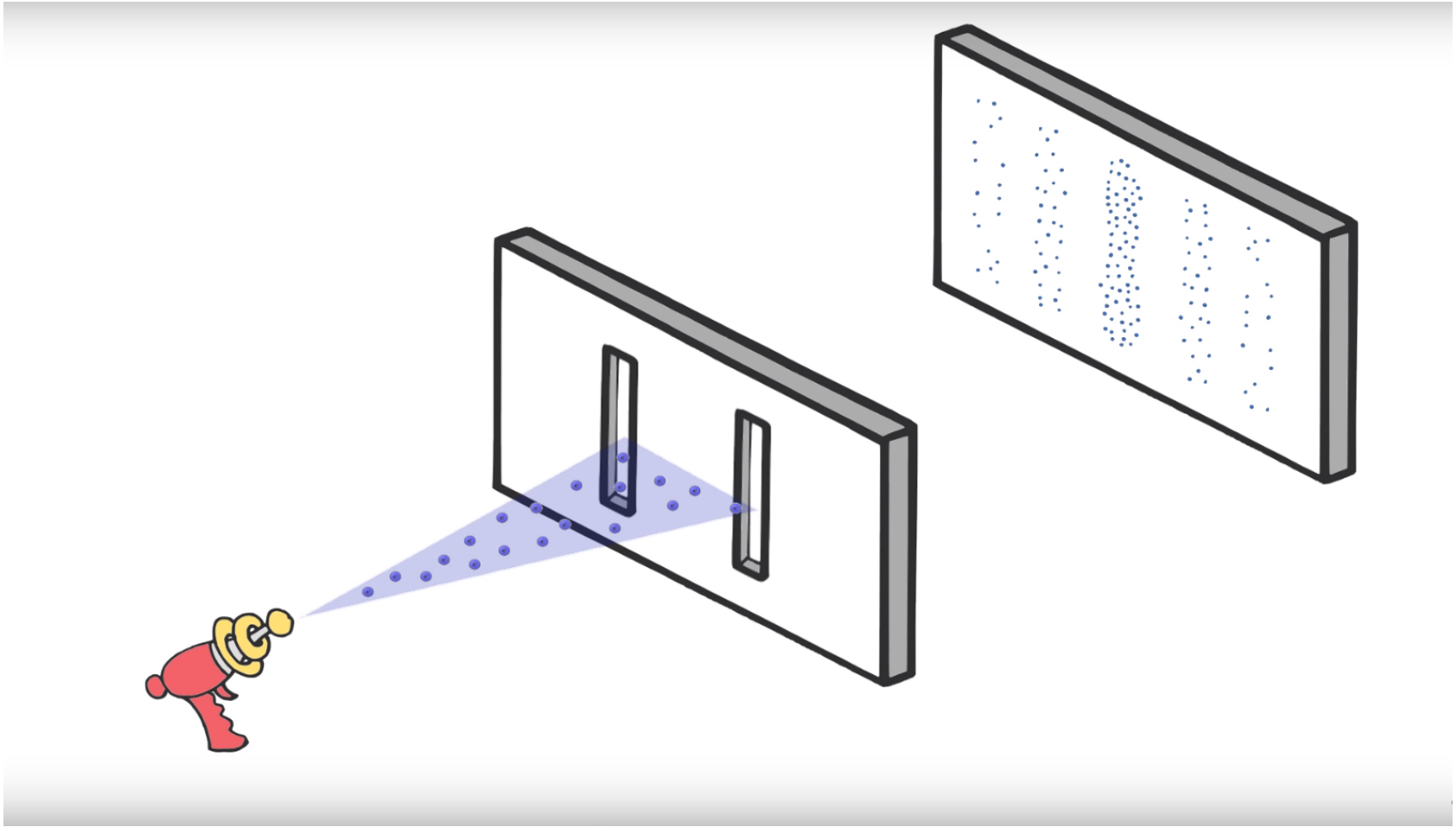
The Double Slit Experiment

Photon beam in one slit

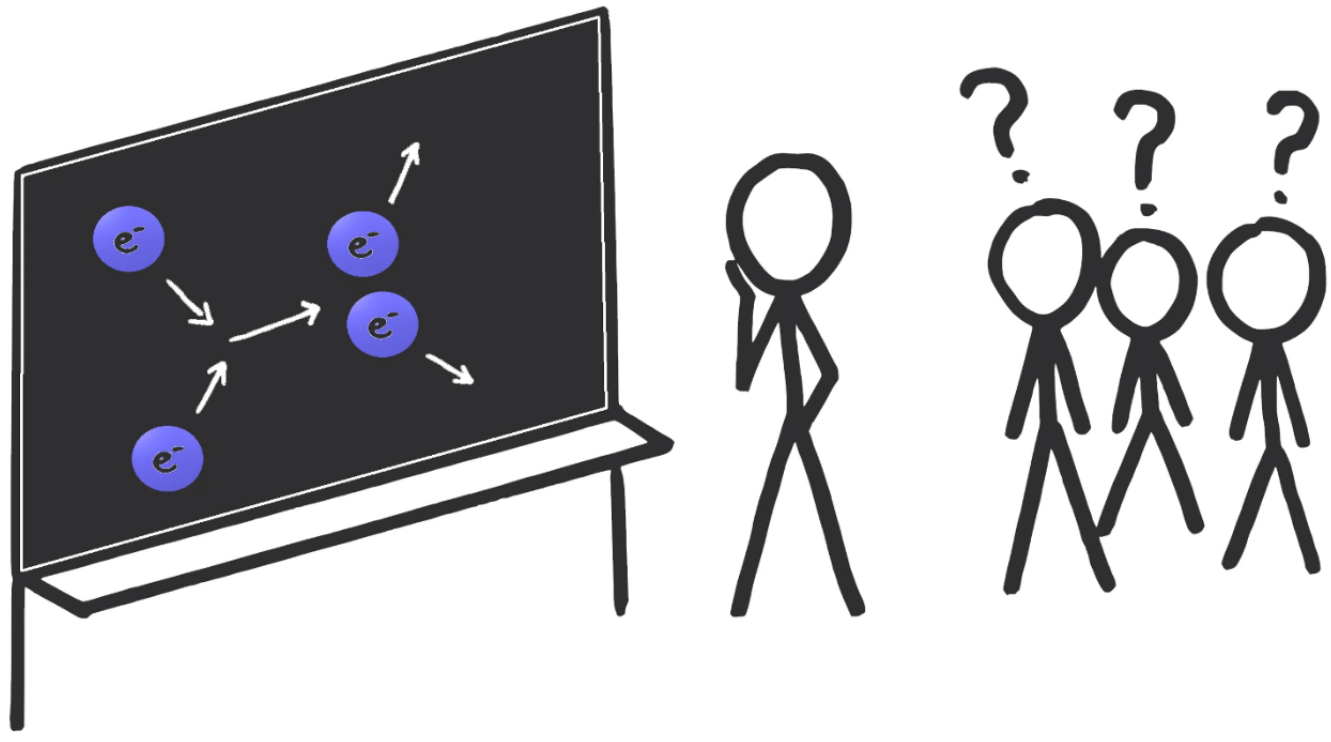


The Double Slit Experiment

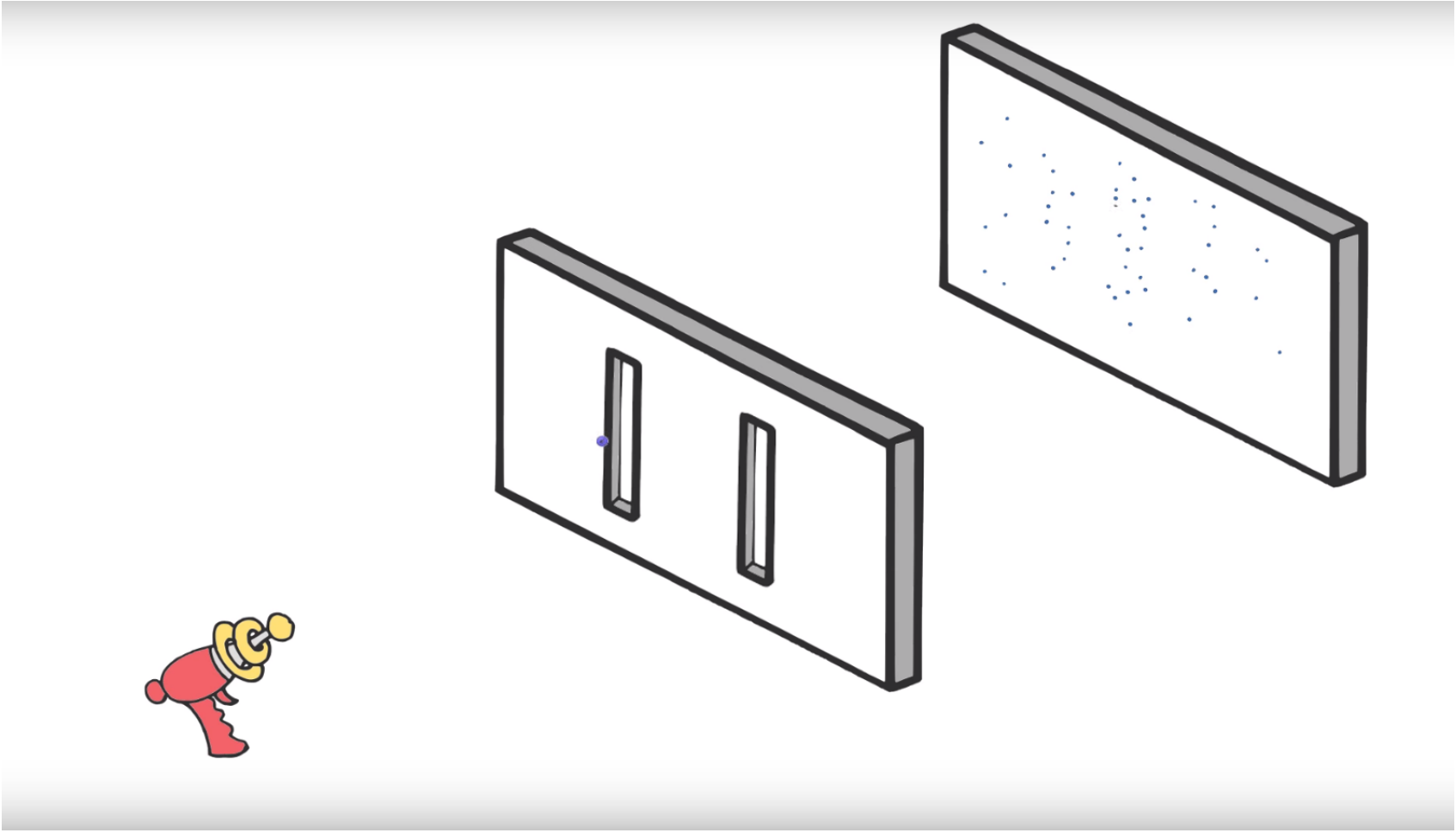
Photon beam in double slit



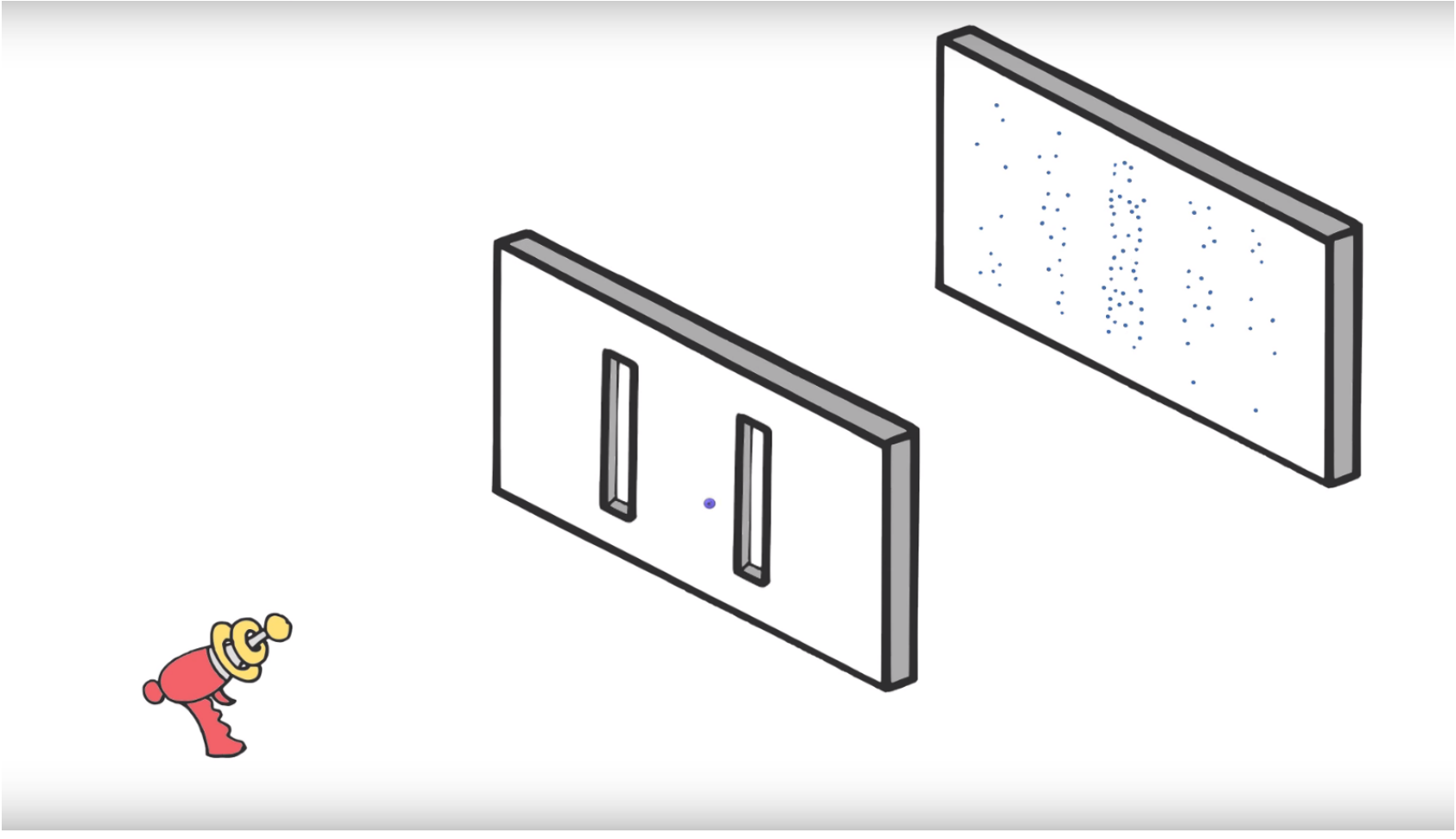
The Double Slit Experiment



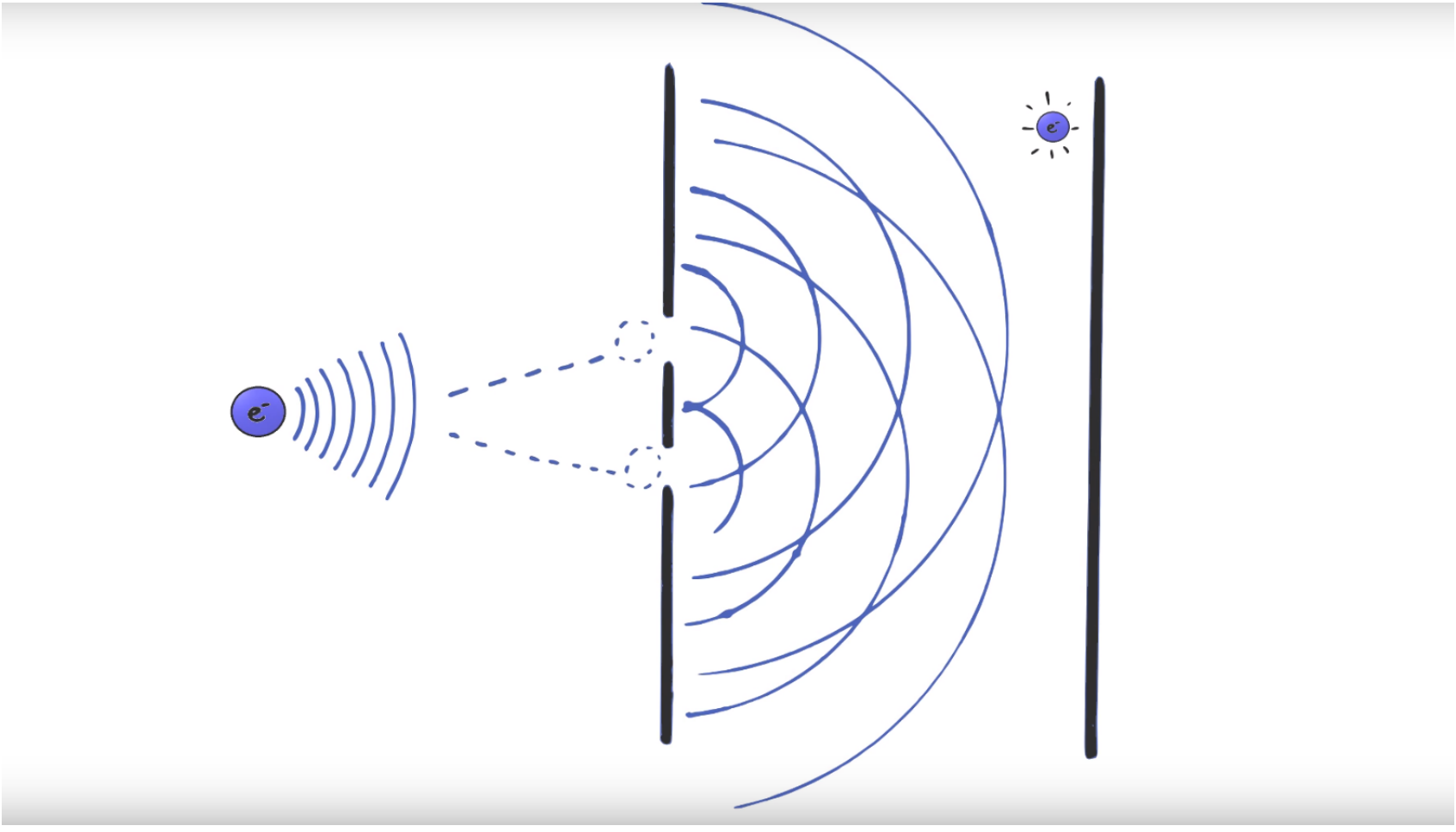
The Double Slit Experiment



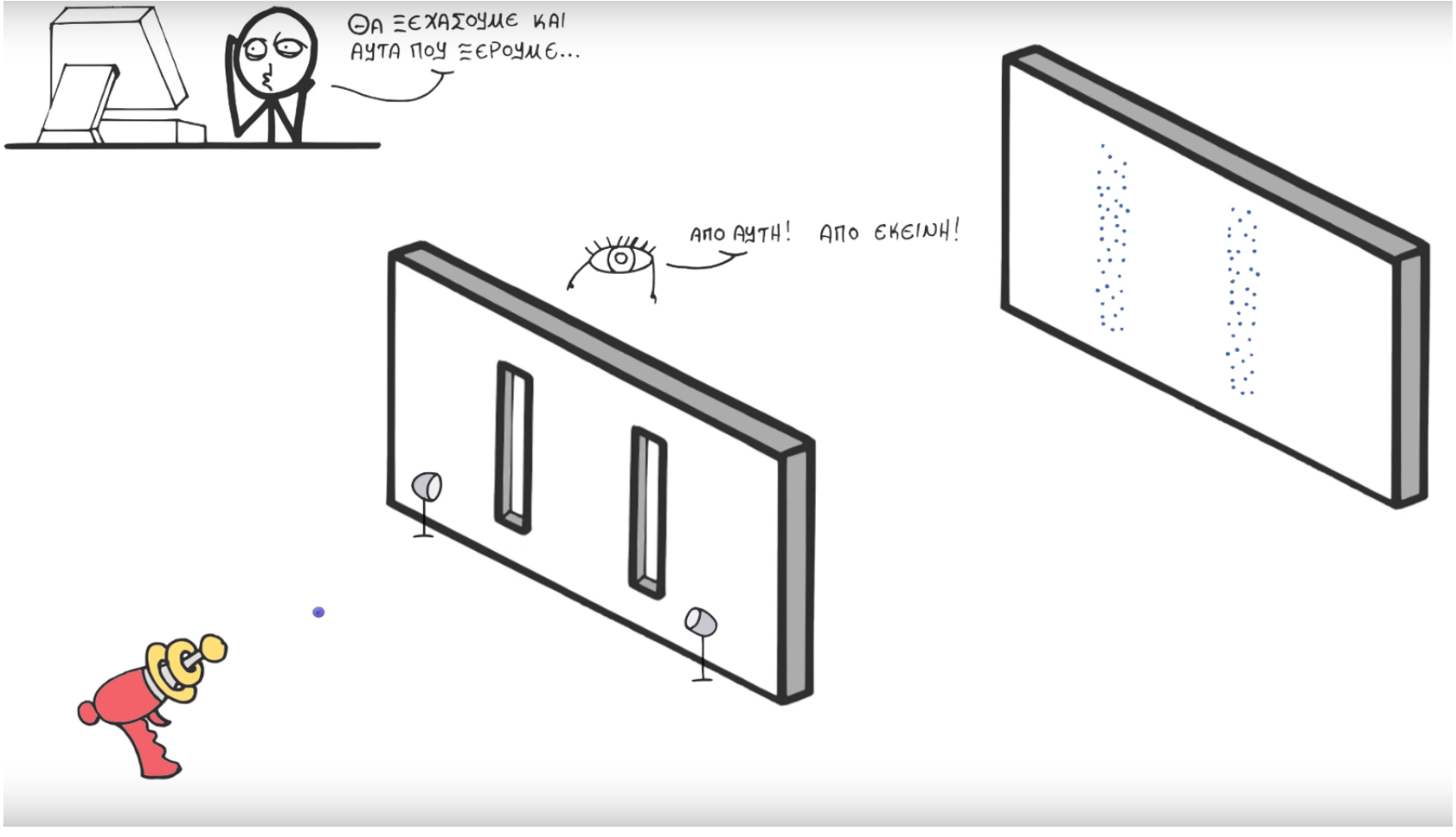
The Double Slit Experiment



The Double Slit Experiment



The Double Slit Experiment



The Double Slit Experiment

"What we observe is not nature itself, but nature exposed to our method of questioning."

Werner Heisenberg

Outline

Classical vs Quantum Bits

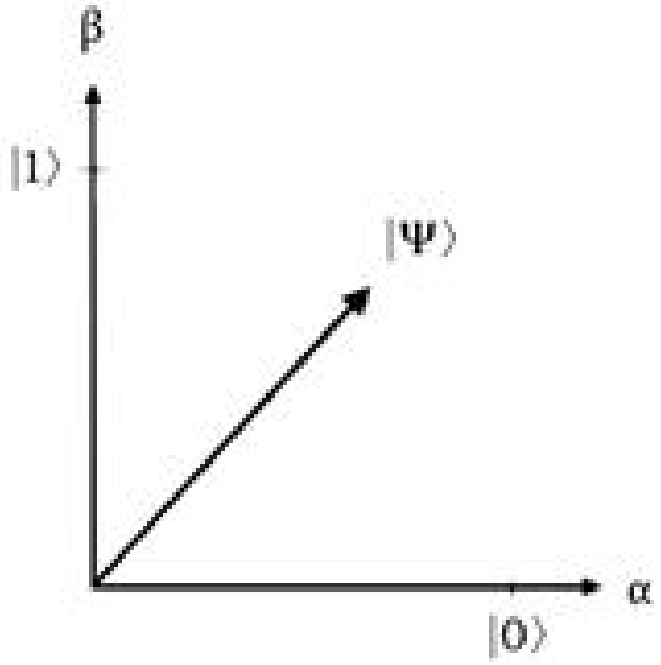
- All classical info can be written down in terms of classical bits.
- All classical computing, communication and cryptographic systems, work with classical bits
- Quantum Crypto works with **qubits**, that are different than classical bits.

$$0 \longrightarrow |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$1 \longrightarrow |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

What do qubits look like?

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle + \beta|1\rangle \in \mathbb{C}^2$$



$|\psi\rangle =$ is a superposition of $|0\rangle$ and $|1\rangle$

What do qubits look like?

- For real vectors $\alpha^2 + \beta^2 = 1$
- Ket $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$
- Bra $\langle\psi| = (|\psi\rangle^*)^T = \begin{pmatrix} \alpha^* \\ \beta^* \end{pmatrix}^T = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix}$
- Inner Product $\langle\psi||\psi\rangle = \langle\psi|\psi\rangle$
- Operations must preserve inner product (unitary operations)
- No-cloning theorem

Many Qubits!

Standard/computational basis:

$x = x_1, ...x_n \in \{0,1\}^n$

$d = 2^n$ possible strings

$$x \longrightarrow |x\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

Quantum State of n qubits:

$|\Psi\rangle = \sum_{x\in\{0,1\}^n} a_x|x\rangle$, $\sum_{x\in\{0,1\}^n} |a|_x^2 = 1$

to sum up:

$|\Psi\rangle \in \mathbb{C}^d$ with $d = 2^n$, $\langle\Psi|\Psi\rangle = 1$

Many Qubits!: Example

Standard basis for two qubits:

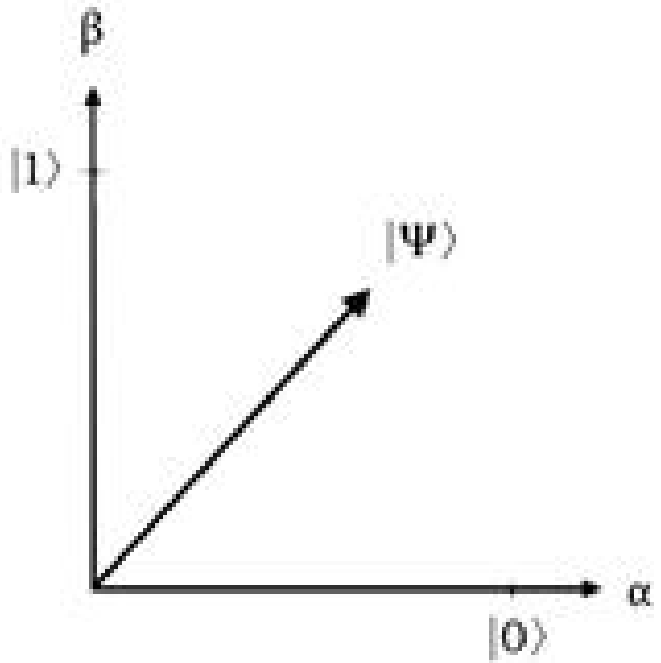
$$|00\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

Equal Superposition:

$$|\Psi\rangle = \tfrac{1}{2}|00\rangle + \tfrac{1}{2}|01\rangle + \tfrac{1}{2}|10\rangle + \tfrac{1}{2}|11\rangle = \ldots\ldots = \tfrac{1}{2}\begin{pmatrix}1\\1\\1\\1\end{pmatrix}$$

$\langle\Psi|\Psi\rangle = 1$, *valid 2-qubit quantum state!*

Measuring qubits

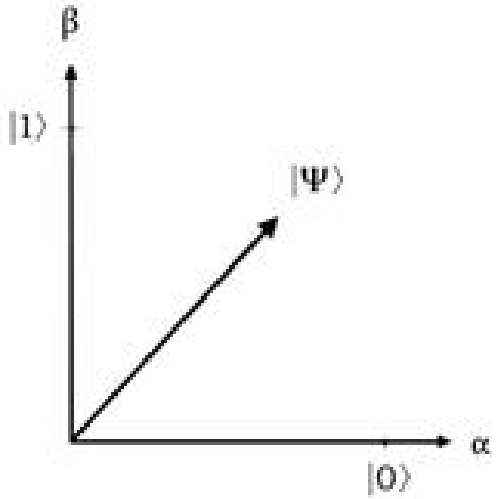


$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|\Psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle + \beta|1\rangle$$

Measuring qubits

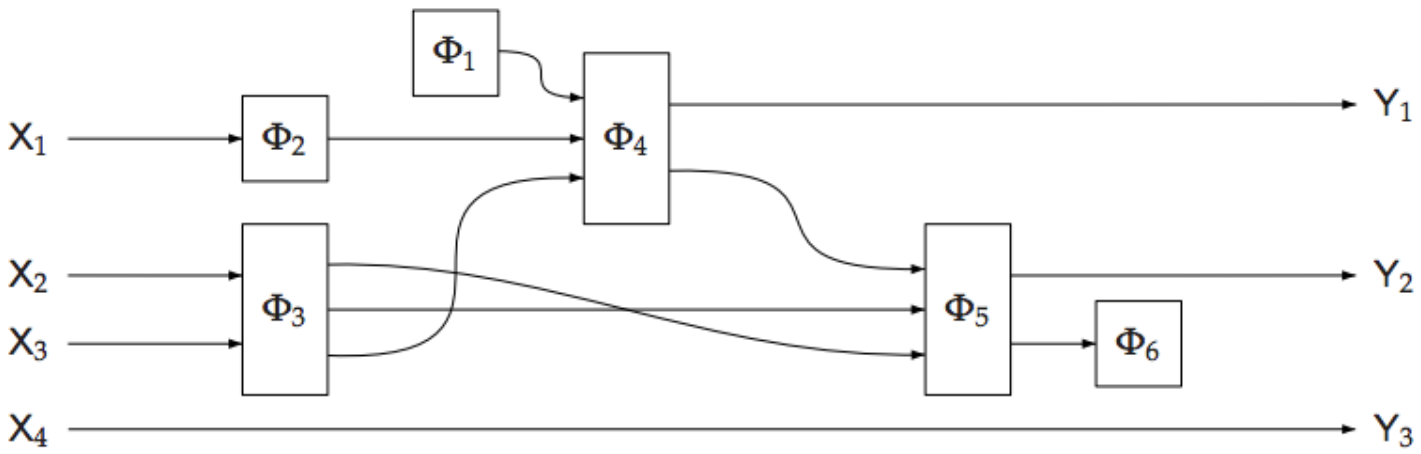


- When we measure, the superposition collapses, we loose information about α and β and we are just in one of the two classic basis states.
- Outcome "$|0\rangle$" (horizontal polarization)
  $p_0 = |\langle\Psi|0\rangle|^2 = |\alpha|^2$
- Outcome "$|1\rangle$" (vertical polarization)
  $p_0 = |\langle\Psi|1\rangle|^2 = |\beta|^2$
- $|\alpha|^2 + |\beta|^2 = 1$

Outline

Quantum Circuits

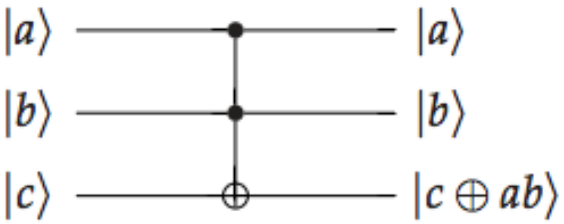
• A model must be chosen when the complexity of quantum computation is studied.
• A quantum circuit is an acyclic network of quantum gates connected by qubit wires. Here is a hypothetical example:



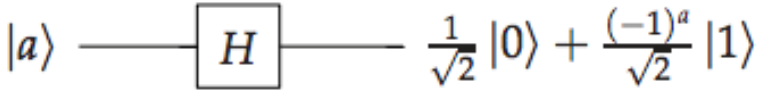
• Any general quantum operation could be considered as a gate but we need to choose a set of allowable gates in order to use the model

Universal set of gates

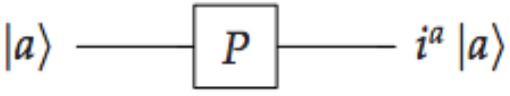
Toffoli gate



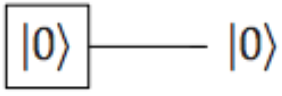
Hadamard gate



Phase-shift gate



Ancillary gate



Erasure gate

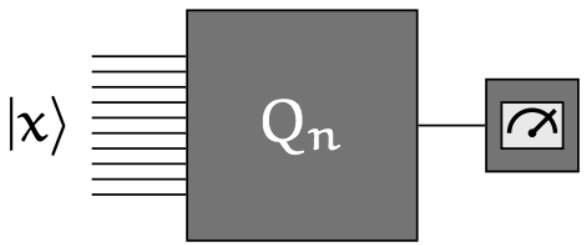
Poly-time quantum algorithms

• In the quantum circuit model, a quantum algorithm Q is described by a family of quantum circuits

$$Q = \{Q_n : n \in \mathbb{N}\}.$$

• Such a family is polynomial-time uniform if there exists a classical algorithm that produces a description of Q_n for each input $n \in \mathbb{N}$, in time polynomial in n

• To run this algorithm on an input x of length n we aply Q_n to $|x\rangle$ and measure the output in the standard basis.



Outline

BQP

• Perhaps the most fundamentally important quantum complexity class is BQP, which stands for Bounded-error Quantum Polynomial time (which we equate with polynomial-time uniform circuit families)

BQP Let $A = (A_{\text{yes}}, A_{\text{no}})$ be a promise problem and let $a, b : \mathbb{N} \to [0,1]$ be functions. Then $A \in \text{BQP}(a,b)$ if and only if there exists a polynomial-time generated family of quantum circuits $Q = \{Q_n : n \in \mathbb{N}\}$, where each circuit Q_n takes n input qubits and produces one output qubit, that satisfies the following properties:

1. if $x \in A_{\text{yes}}$ then $\Pr[Q \text{ accepts } x] \geq a(|x|)$, and
2. if $x \in A_{\text{no}}$ then $\Pr[Q \text{ accepts } x] \leq b(|x|)$.

The class BQP is defined as $\text{BQP} = \text{BQP}(2/3, 1/3)$.

• A wide range of values can be substituted for $2/3$ without changing the class.

Relation of BQP to classical classes

$$BPP \subseteq BQP \subseteq PP.$$

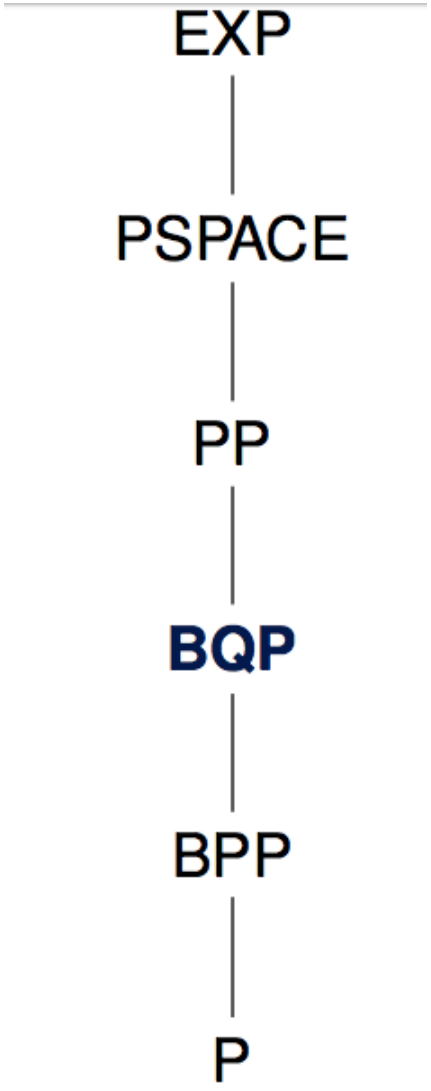
The containment $BPP \subseteq BQP$ is obvious if you believe the claims about universal gate sets from a few slides ago. . .
. . . classical Boolean logic gates (including fanouts) and randomly generated bits can be simulated with quantum circuits.

- There are multiple ways to prove the containment $BQP \subseteq PP$

Intuitive proof: unbounded error probabilistic computations can simulate interference in quantum computations. (E.g, run two probabilistic processes, and condition on obtaining the same outputs.)

Abstract proof: PP computations can simulate exponential-size matrix multiplication problems of certain types.

Diagram of Classes



Outline

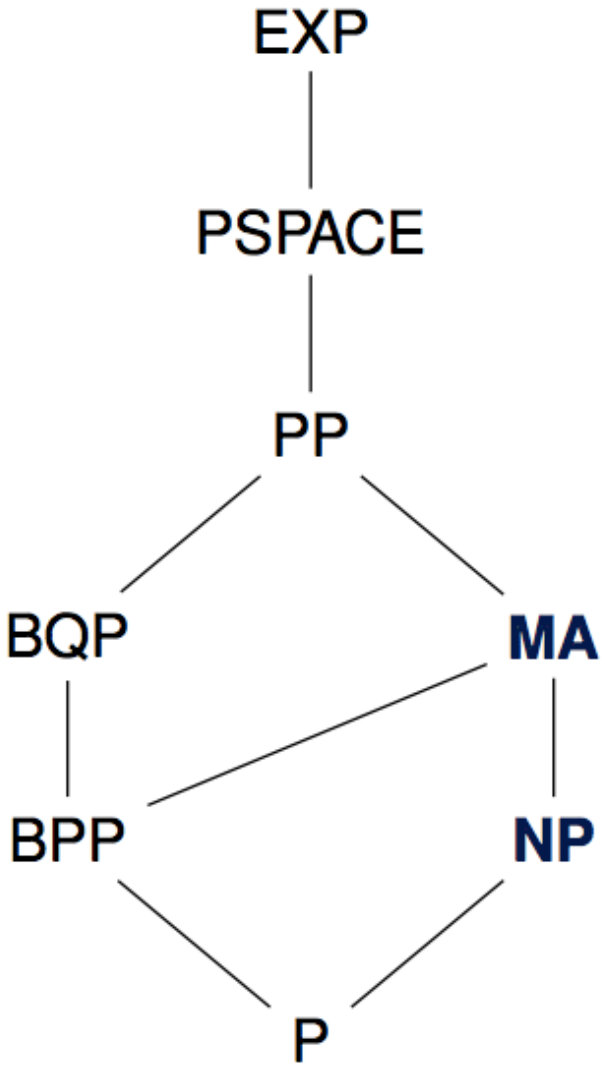
MA

• The complexity class MA is defined similarly to NP, except that the verification procedure is probabilistic.

MA A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in MA if and only if there exists a polynomial-bounded function p and a probabilistic polynomial-time Turing machine M with the following properties. For every string $x \in A_{\text{yes}}$, it holds that $\Pr[M \text{ accepts } (x, y)] \geq \frac{2}{3}$ for some string $y \in \Sigma^{p(|x|)}$; and for every string $x \in A_{\text{no}}$, it holds that $\Pr[M \text{ accepts } (x, y)] \leq \frac{1}{3}$ for all strings $y \in \Sigma^{p(|x|)}$.

• MA stands for Merlin-Arthur, and is one of multiple complexity classes represented by Arthur-Merlin games.

Diagram of Classes



QMA: a quantum analogue of NP

• One way to define a quantum computational analogue of NP (or MA, really) is to extend the definition in two ways:

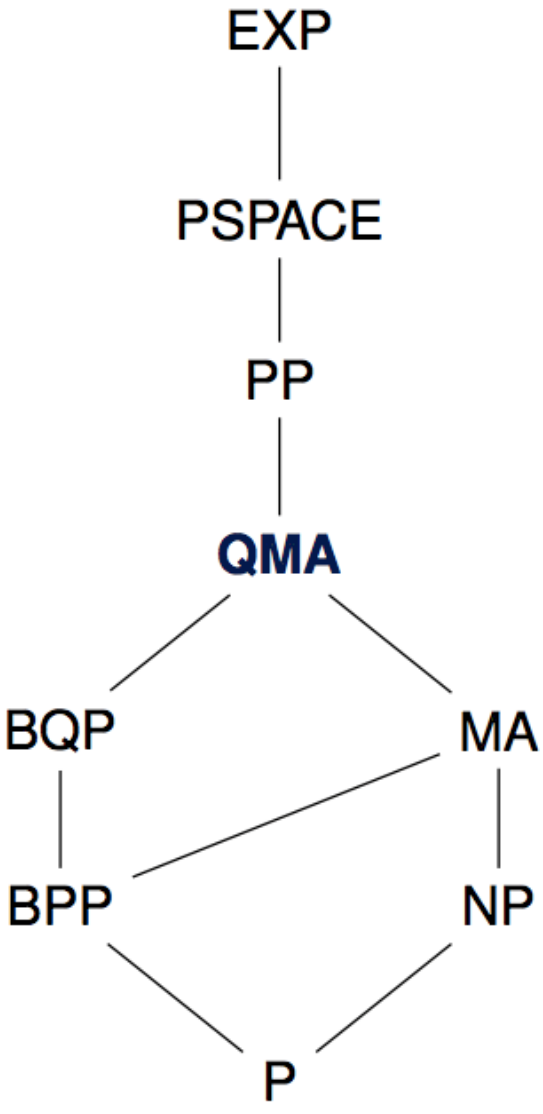
1. Allow the verification procedure to be a quantum computation.
2. Allow the proof (or certificate) to be a quantum state.

QMA Let $A = (A_{\text{yes}}, A_{\text{no}})$ be a promise problem, let p be a polynomial-bounded function, and let $a, b : \mathbb{N} \to [0,1]$ be functions. Then $A \in \text{QMA}_p(a,b)$ if and only if there exists a polynomial-time generated family of circuits $Q = \{Q_n : n \in \mathbb{N}\}$, where each circuit Q_n takes $n + p(n)$ input qubits and produces one output qubit, with the following properties:

1. *Completeness.* For all $x \in A_{\text{yes}}$, there exists a $p(|x|)$-qubit quantum state ρ such that $\Pr[Q \text{ accepts } (x,\rho)] \geq a(|x|)$.
2. *Soundness.* For all $x \in A_{\text{no}}$ and all $p(|x|)$-qubit quantum states ρ it holds that $\Pr[Q \text{ accepts } (x,\rho)] \leq b(|x|)$.

Also define $\text{QMA} = \bigcup_p \text{QMA}_p(2/3, 1/3)$, where the union is over all polynomial-bounded functions p.

Diagram of Classes



Complete promise problem for QMA

There are several problems known to be complete for QMA (with respect to classical polynomial-time many-to-one reductions).

THE k-LOCAL HAMILTONIAN PROBLEM

Input: A collection $H_1, \ldots, H_m$ of k-local Hermitian matrices with entries indexed by strings of length n and satisfying $\|H_j\| \leq 1$ for $j = 1, \ldots, m$.

Yes: There exists an n-qubit quantum state $|\psi\rangle$ such that $\langle\psi|H_1 + \cdots + H_m|\psi\rangle \leq -1$.

No: For every n-qubit quantum state $|\psi\rangle$ it holds that $\langle\psi|H_1 + \cdots + H_m|\psi\rangle \geq 1$.

The 2-local Hamiltonian problem is complete for QMA

Outline

Group-theoretic problems

• Let G be a finite group whose elements can be represented (uniquely) by binary strings of a given length n.
• Efficient computation of group operations: Given two elements $g, h \in G$, it is assumed that the group operations can be efficiently implemented by quantum circuits:
1. Multiplication: $|g\rangle|h\rangle \to |g\rangle|gh\rangle$.
2. Inverse: $|g\rangle \to |g^{-1}\rangle$.
• **Abstraction:**
It is sometimes helpful to view such a group as a black box group; the group operations are performed by a black box (or group oracle), and string representatives of elements are independent of group structure.
For those not familiar with groups, you could think of G as the collection of invertible $n \times n$ matrices with entries in $\{0, ..., p-1\}$ (for prime p), assuming all arithmetic is done modulo p.

Group membership

Consider the **group membership** problem:

Input: Group elements $g_1, \ldots, g_k$ and h of G.

Yes: $h \in \langle g_1, \ldots, g_k \rangle$.

No: $h \notin \langle g_1, \ldots, g_k \rangle$.

Notation: $\langle g_1, \ldots, g_k \rangle$ is the subgroup of G generated by $g_1, \ldots, g_k$.

(This is every element that can be obtained by multiplying any number of elements from $\{g_1, \ldots, g_k\}$ in any order, any number of times.)

The group membership problem is in NP.

A given $h \in \langle g_1, \ldots, g_k \rangle$ might require an exponentially long product of elements in $\{g_1, \ldots, g_k\}$ to be reached...

...but the **reachability lemma** of Babai and Szemerédy implies that there is a short **straight-line program** generating h from $g_1, \ldots, g_k$.

Group non-membership

Input: Group elements $g_1, \ldots, g_k$ and h of G.

Yes: $h \notin \langle g_1, \ldots, g_k \rangle$.

No: $h \in \langle g_1, \ldots, g_k \rangle$.

Theorem. The group non-membership problem is in QMA.

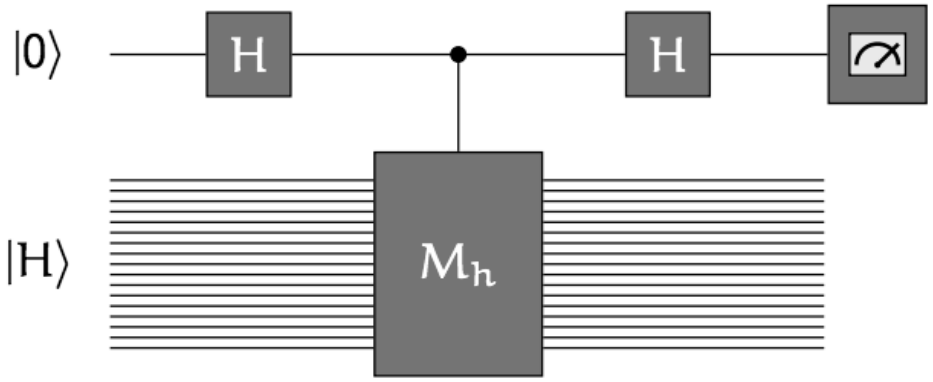
The idea is simple: for $H = \langle g_1, \ldots, g_k \rangle$, the quantum proof that $h \notin H$ will be the state

$$|H\rangle = \frac{1}{\sqrt{|H|}} \sum_{a \in H} |a\rangle .$$

Let us suppose momentarily that we have a copy of the state

$$|H\rangle = \frac{1}{\sqrt{|H|}} \sum_{a \in H} |a\rangle .$$

Consider what happens when we run the following algorithm:

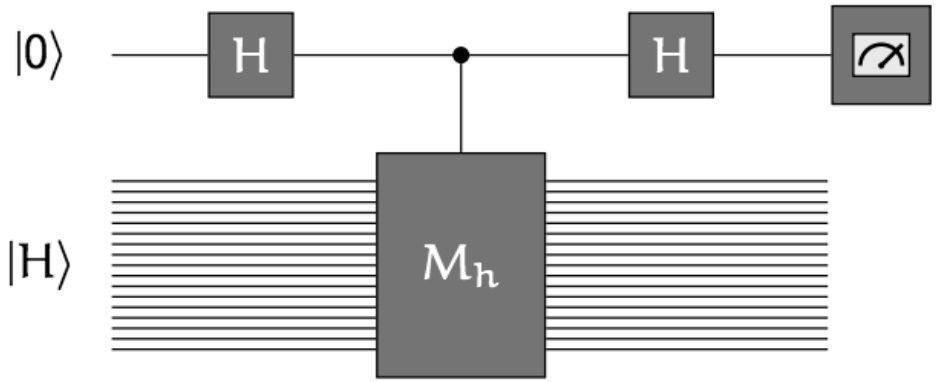


The controlled-multiplication gate $\Lambda(M_h)$ operates as

$$\Lambda(M_h) : |0\rangle |a\rangle \mapsto |0\rangle |a\rangle \qquad \text{and} \qquad \Lambda(M_h) : |1\rangle |a\rangle \mapsto |1\rangle |h \cdot a\rangle$$

NO-input case

Consider first the case of a NO-input: $h \in H = \langle g_1, \ldots, g_k \rangle$.



Given that $h \in H$, we have

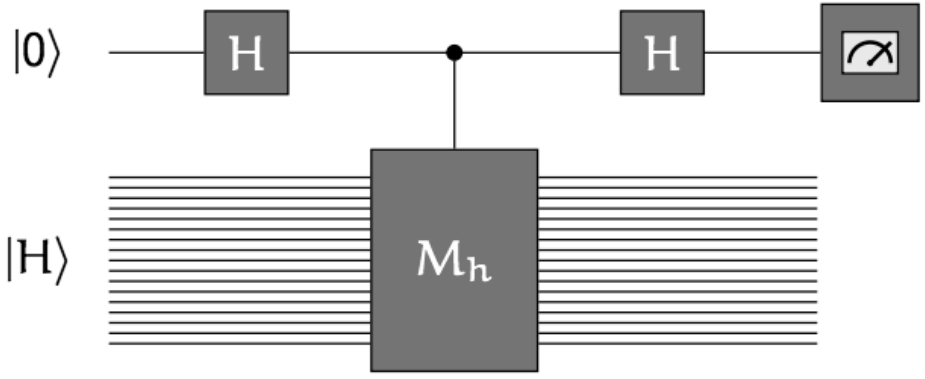
$$M_h |H\rangle = |hH\rangle = |H\rangle ,$$

so the controlled-multiplication operation has no effect.

As $H^2 |0\rangle = |0\rangle$, the measurement will always result in the outcome 0 (with certainty).

YES-input case

Now consider the case of a YES-input: $h \notin H = \langle g_1, \ldots, g_k \rangle$.



Given that $h \notin H$, we have

$$M_h |H\rangle = |hH\rangle \perp |H\rangle ,$$

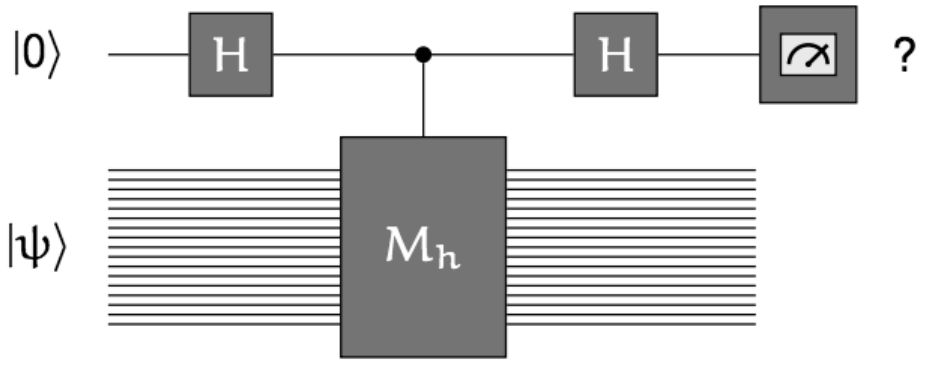
so the controlled-multiplication operation acts just like a measurement of the top qubit.

The reduced state of the top qubit will be **totally mixed** after the multiplication: the measurement result will be a **uniform random bit**.

But we can't trust the proof...

There is a problem, however...we cannot trust that the given quantum state $|\psi\rangle$ is equal to $|H\rangle$.

For an arbitrary state $|\psi\rangle$, any behavior is possible:

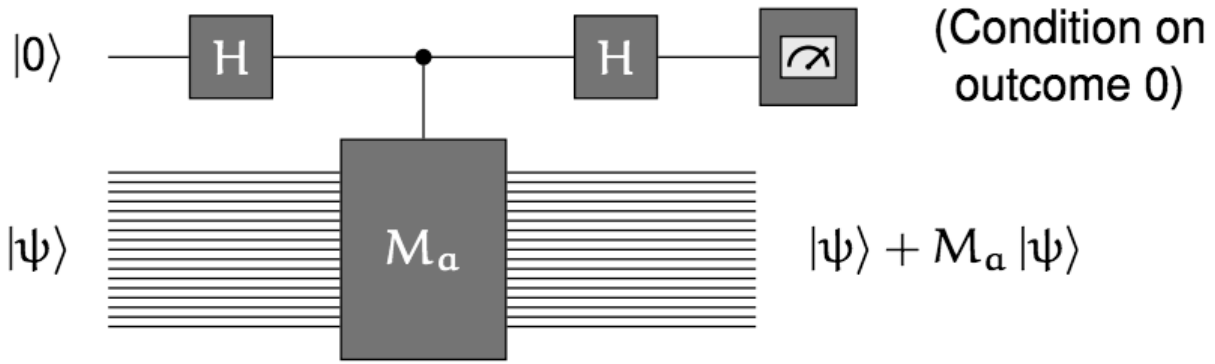


Solution. Before running the membership test with h, run the test with a (suitable) **random choice** of elements $a_1, \ldots, a_k \in H$ in place of h.

If non-membership is indicated for any of the test inputs, immediately reject: the state $|\psi\rangle$ must be invalid. Otherwise, run the membership test for h on the **resulting state**.

Modified proof

Consider what happens when the membership test is run for some element $a \in H$, conditioned on seeing the output 0:



After repeating with $a_1, \ldots, a_k$, the resulting state will be close to

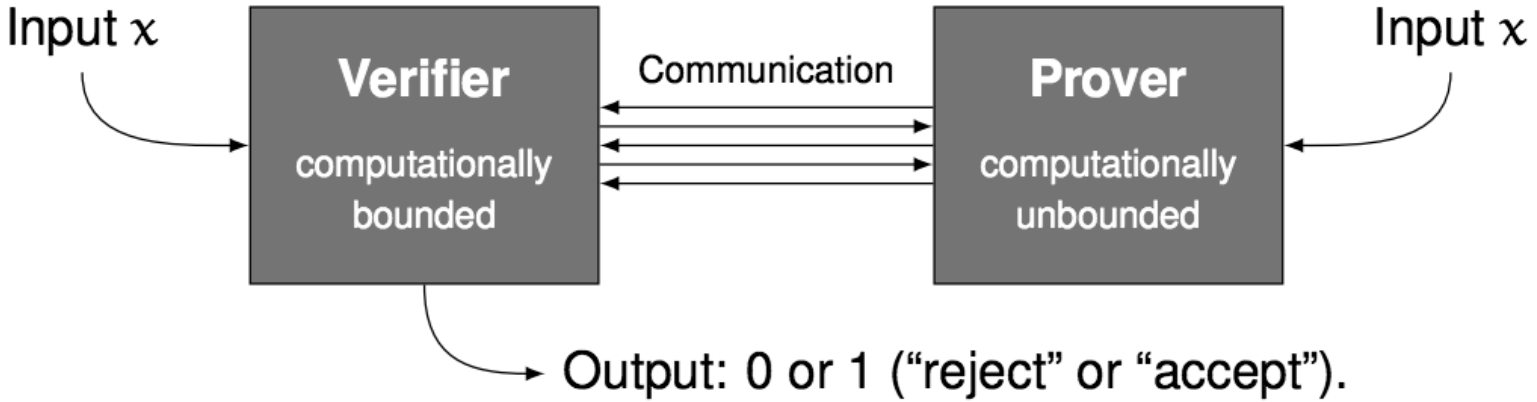
$$\sum_{a \in H} M_a |\psi\rangle \quad \text{(normalized)}.$$

This state is now suitable for the membership test on h (because it is nearly invariant under left multiplication by elements of H).

Outline

Interactive proof systems

The notion of efficient verification can be extended to an **interactive** setting. **Interactive proof systems** model this situation.



To say that a promise problem A has an interactive proof system means that there exists a verifier meeting two conditions:

Completeness: For every input $x \in A_{\text{yes}}$, there must exist a prover strategy causing the verifier to accept with high probability.

Soundness: For every input $x \in A_{\text{no}}$, all prover strategies must cause the verifier to reject with high probability.

Complexity classes for interactive proofs

Several variants of classical interactive proof systems have been studied, and many results are known about these models.

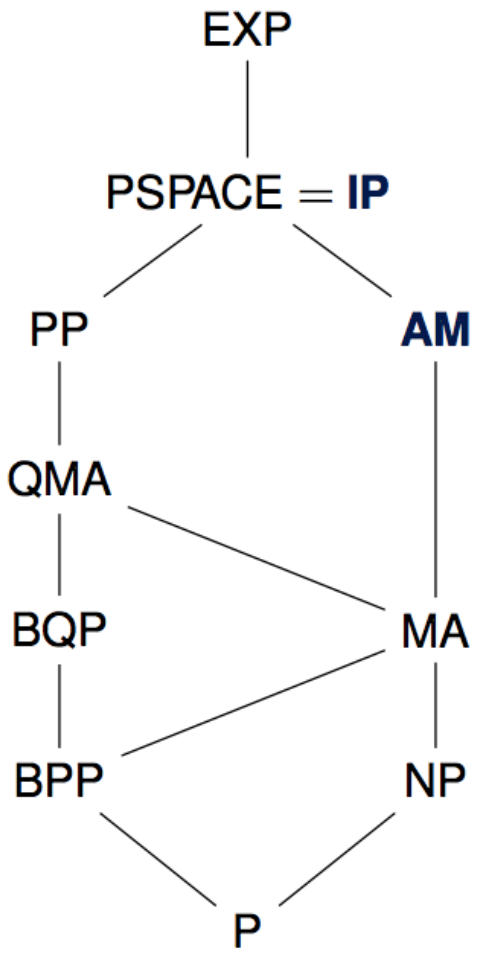
Two fundamental complexity classes based on these models:

AM	The class of promise problems having classical interactive proof systems with a **constant number of messages** exchanged between the prover and verifier.
IP	The class of promise problems having classical interactive proof systems (allowing **any polynomial number of messages** to be exchanged between the prover and verifier).

It is known that IP = PSPACE.

[Lund, Fortnow, Karloff, & Nisan 1990; Shamir 1990]

Both classes are highly robust with respect to choices of error bounds.

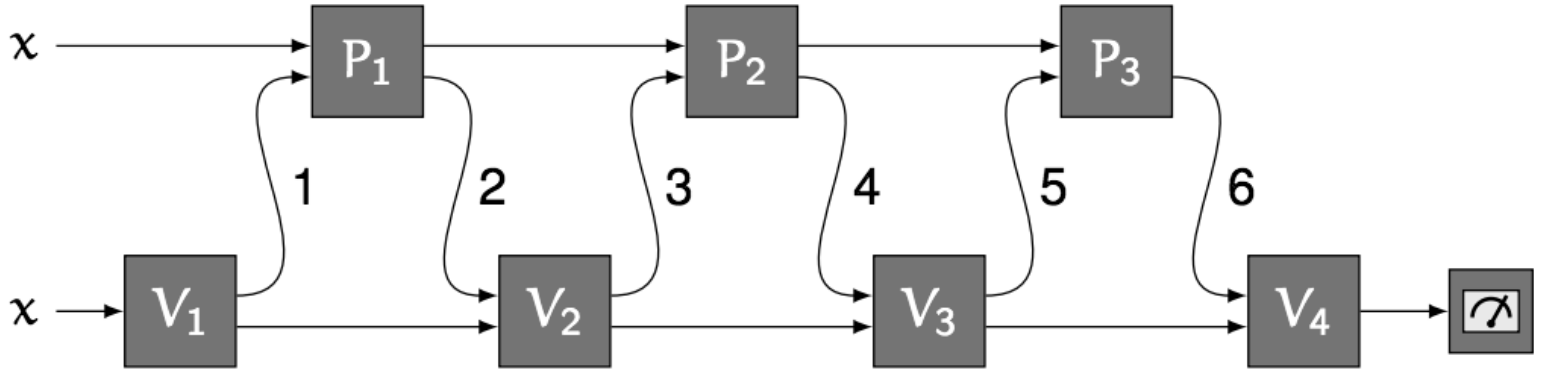

EXP
PSPACE = IP
PP
AM
QMA
BQP
MA
BPP
NP
P

Quantum interactive proof systems

The **quantum interactive proof system** model works exactly the same as the classical model, except that the prover and verifier may exchange and process quantum information.

General assumptions and notions of completeness and soundness are unchanged. . .

The model may be formalized in terms of quantum circuits. An illustration of an interaction:



(There are six messages in this example.)

QIP

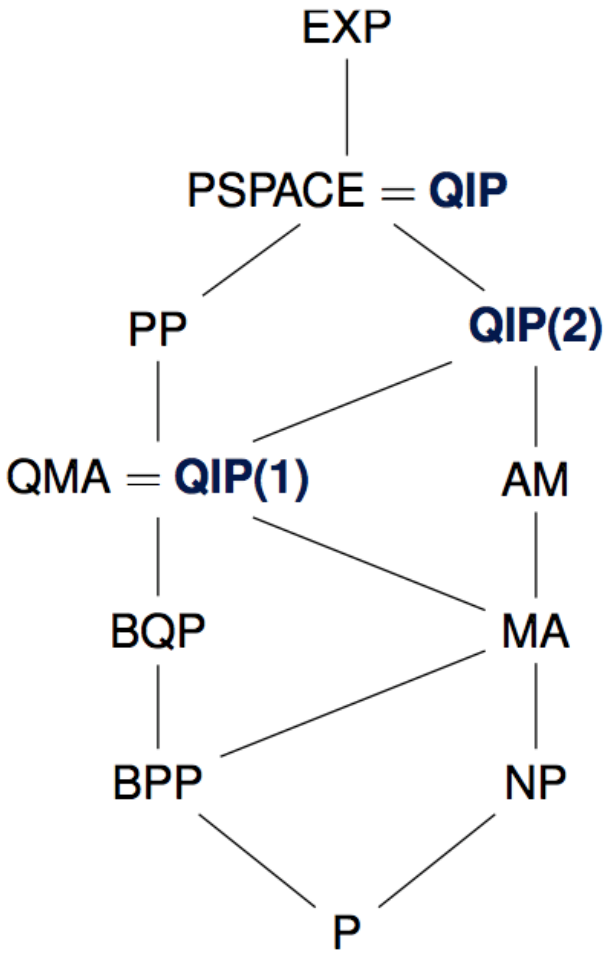
We define complexity classes based on quantum interactive proofs as follows:

QIP	The class of promise problems having quantum interactive proof systems (allowing any polynomial number of messages to be exchanged between the prover and verifier).
QIP(m)	The class of promise problems having quantum interactive proof systems, where at most m messages are exchanged in total.

It holds that

$$\mathrm{QIP}(3) = \mathrm{QIP} = \mathrm{PSPACE};$$

quantum interactive proof systems are no more powerful than classical ones, but offer a reduction in the number of required required.


EXP
PSPACE = QIP
PP
QIP(2)
QMA = QIP(1)
AM
BQP
MA
BPP
NP
P

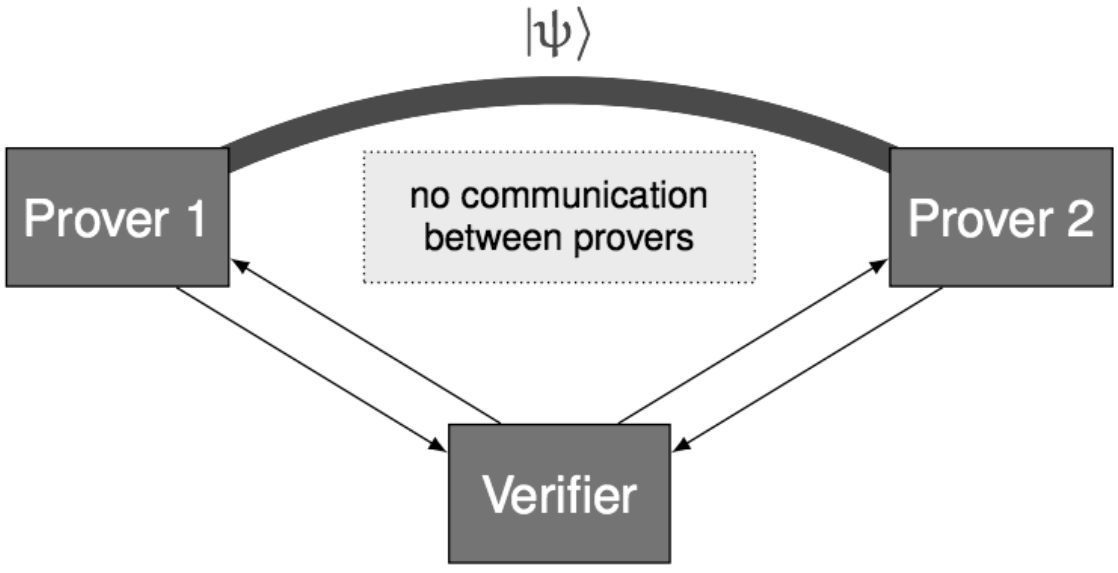
Other topics in quantum complexity theory

There are many other topics in quantum complexity that have not been discussed in this talk. Examples include:

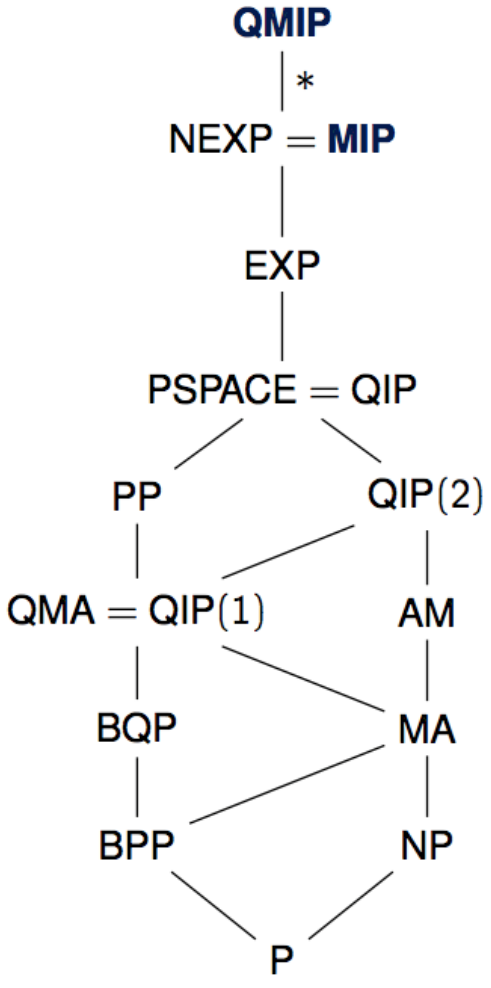
- Quantum query complexity and quantum communication complexity.
- Hamiltonian complexity (quantum PCP theorem, relation to area laws, ...).
- Other variants of QMA and QIP (multiple-Merlin QMA, competing prover and zero-knowledge quantum interactive proofs, ...).
- Quantum advice.
- BQP versus the polynomial-time hierarchy.
- Complexity-theoretic aspects of limited quantum models (such as linear optical quantum computers, the one-clean-qubit model, matchgate circuits, ...).
- Bounded depth and bounded space quantum complexity classes.

Open problem: upper-bounding entangled provers

Proving upper bounds on **entangled provers** that cannot communicate is a major challenge.



QMIP The class of promise problems having multi-prover quantum interactive proof systems.



* Announced by Thomas Vidick (joint work with Tsuyoshi Ito) in April 2012.

References

1. John Watrous, Quantum Computational Complexity.
2. Scott Aaronson, Quantum Complexity Theory Lecture Notes, MIT.