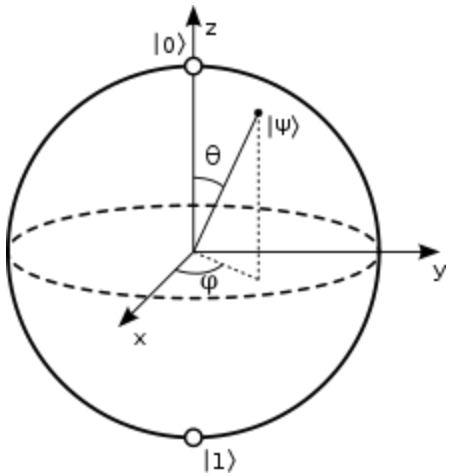
Intro to Quantum Computing

Introduction



Slides from Georgios Stamouli

Administrative info

- Instructor: Menica Dibenedetto
- Tutor: Shi Qiu shi.qiu@maastrichtuniversity.nl
- Communication: domenica.dibenedetto@maastrichtuniversity.nl
- Office: C4.032
- Office hours: by appointment (for small questions: open door -> please do come in!)

Administrative info

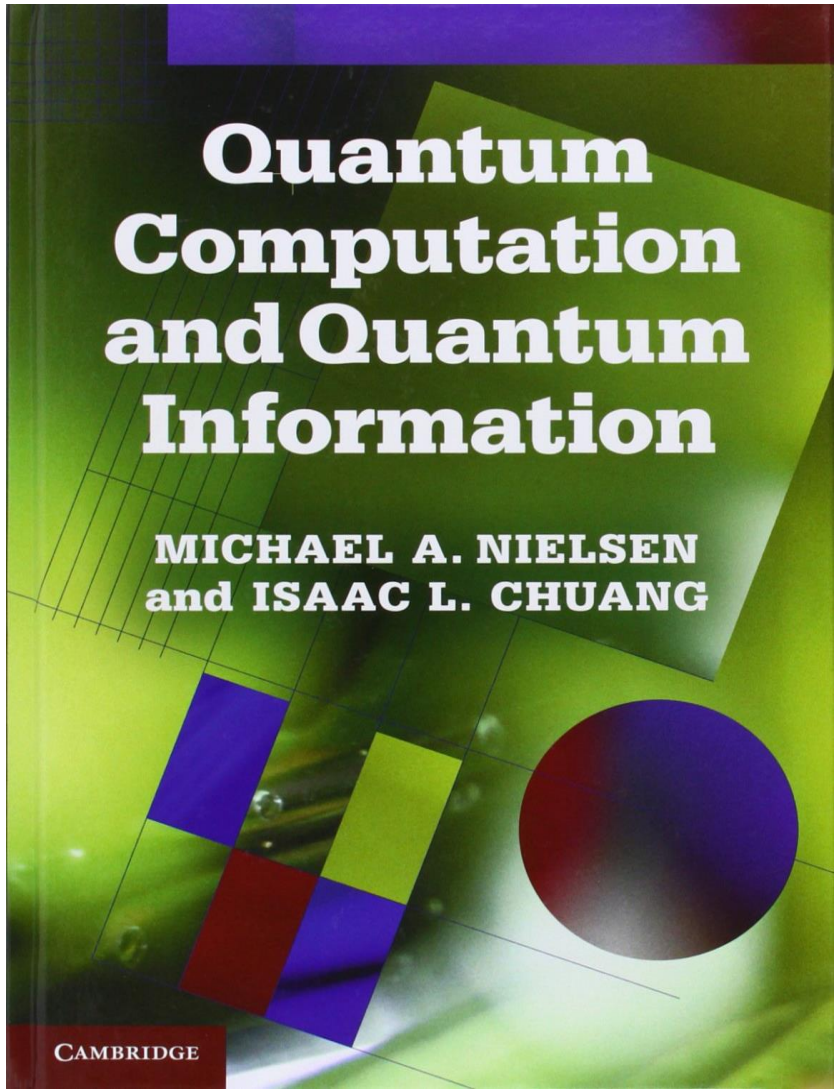
- 17 appointments (lectures/tutorials/Q&A)
- Broadly split into four themes:
  - Mathematics of Qbits
  - Quantum Entanglement & Bell's Inequalities
  - Quantum Logic and Circuits
  - Quantum Algorithms, Protocols and Applications (Cryptography etc.)
- Final Exam: Closed book, for 100% of the final grade.
- Periodically a set of exercises.

Knowledge

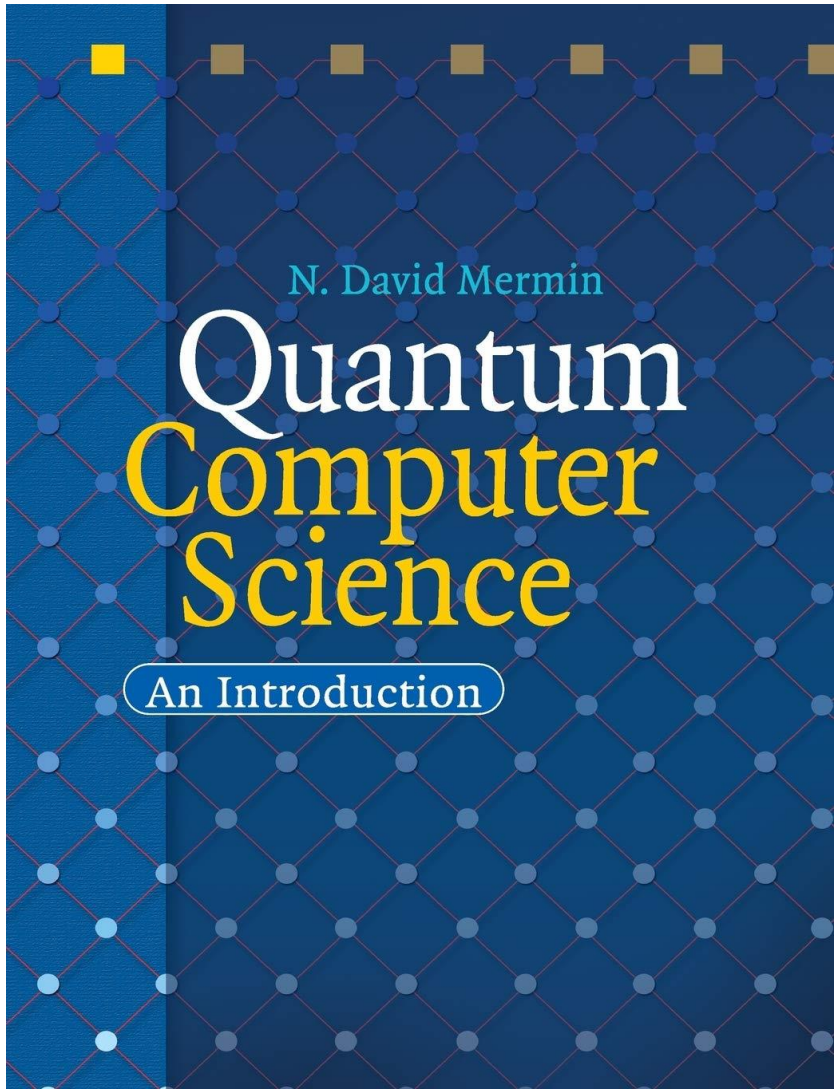
- Desired prior Knowledge:
  - Very good knowledge of *Linear Algebra* (we will cover the basic tools in a vocabulary appropriate for manipulating Qbits but you should already be familiar with concepts of Vector Spaces, Bases, Orthogonality, Inner Products, Linear Transformations etc.)
- Algorithmic thinking will help you (but it is not strictly necessary)
- *No prior knowledge of Quantum Physics is assumed. We will build all concepts (Superposition, Entanglement, etc.) from first principles.*

Sources

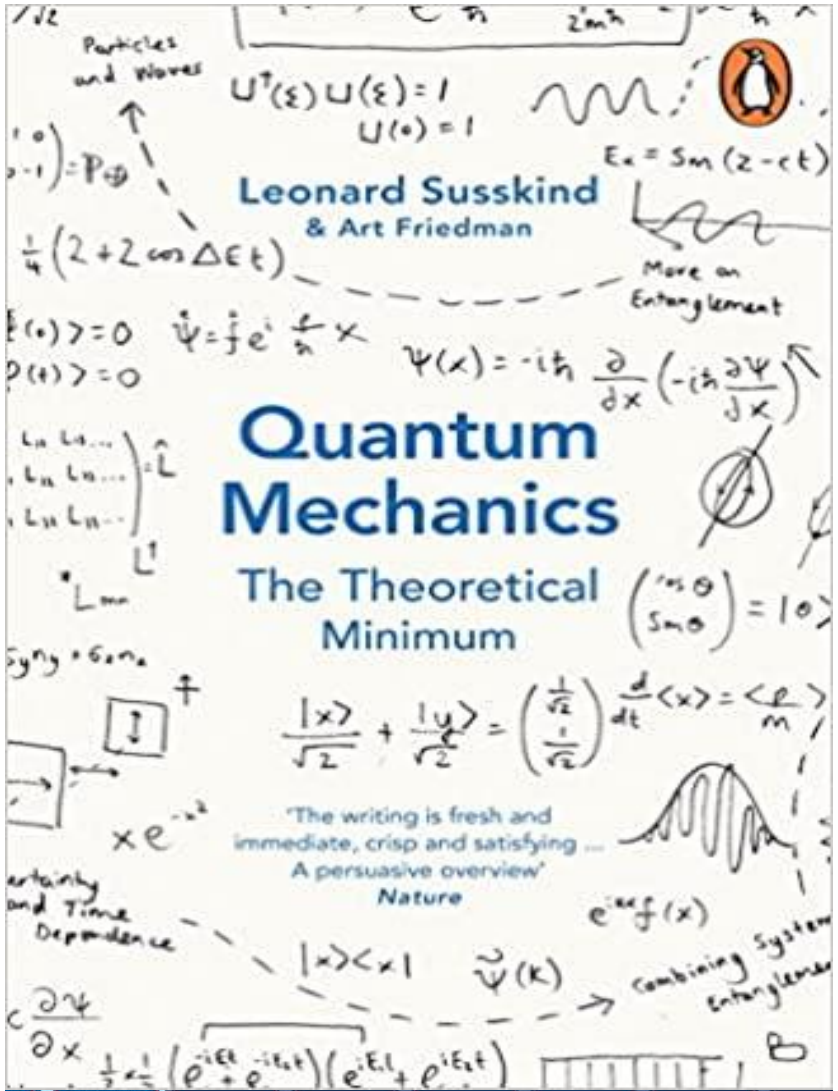
Sources


Quantum Computation and Quantum Information
MICHAEL A. NIELSEN and ISAAC L. CHUANG
CAMBRIDGE

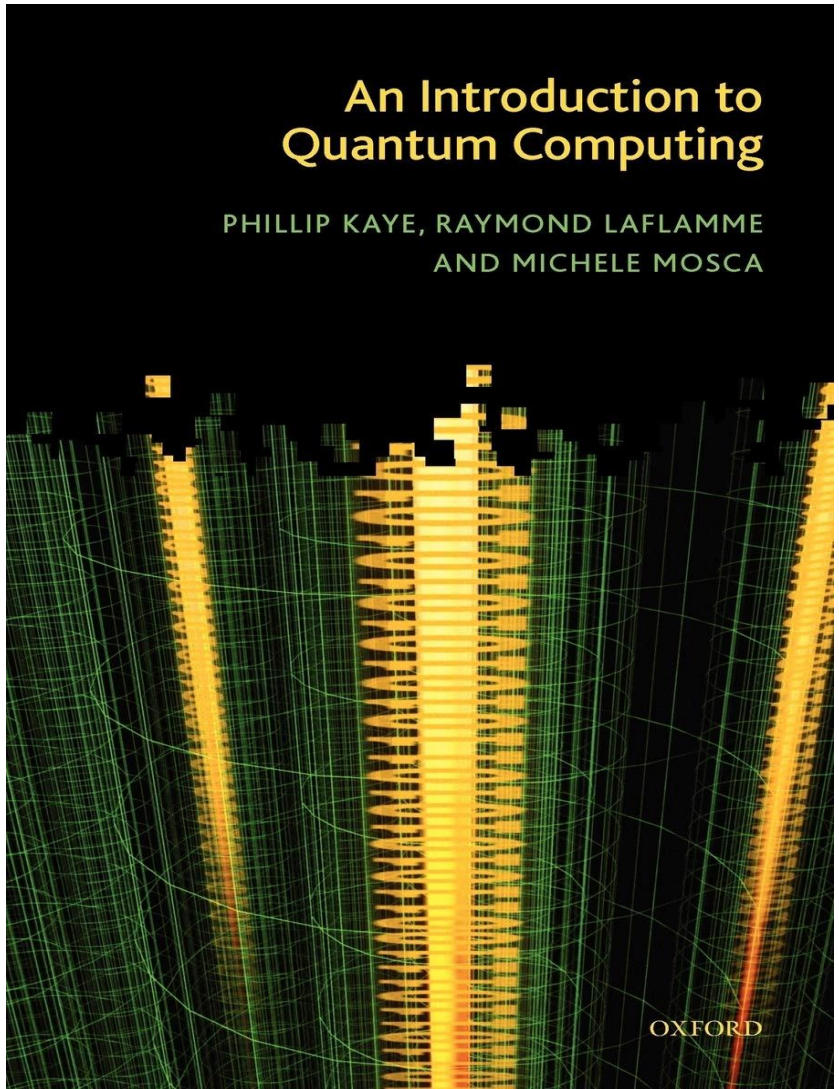
Sources



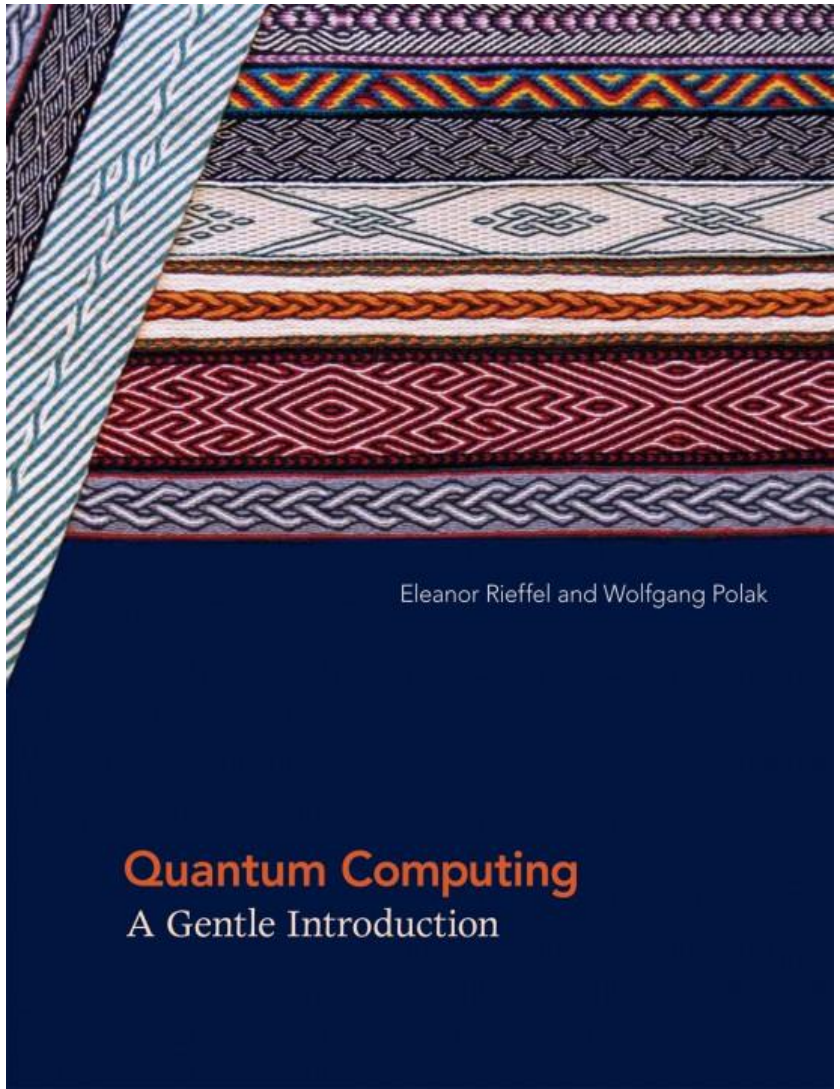
Sources


Particles and Waves
Leonard Susskind
& Art Friedman
More on Entanglement
Quantum Mechanics
The Theoretical Minimum
'The writing is fresh and immediate, crisp and satisfying ... A persuasive overview'
Nature
Combining Systems

Sources


An Introduction to
Quantum Computing
PHILLIP KAYE, RAYMOND LAFLAMME
AND MICHELE MOSCA
OXFORD

Sources


Eleanor Rieffel and Wolfgang Polak
Quantum Computing
A Gentle Introduction

What this course is about

What this course is about

- To understand the nature of **Qbit**.

What this course is about

- To understand the nature of **Qbit**.
- To understand the principles of ***Quantum Mechanics*** (quantum interference, superposition etc.) that help us design Quantum Algorithms.

What this course is about

- To understand the nature of **Qbit**.
- To understand the principles of ***Quantum Mechanics*** (quantum interference, superposition etc.) that help us design Quantum Algorithms.
- To built intuition about the ***Quantum Computational model***.

What this course is about

- To understand the nature of **Qbit**.
- To understand the principles of ***Quantum Mechanics*** (quantum interference, superposition etc.) that help us design Quantum Algorithms.
- To built intuition about the ***Quantum Computational model***.
- To understand what problems ***might*** benefit from a Quantum Computer.

What this course is about

- To understand the nature of **Qbit**.
- To understand the principles of ***Quantum Mechanics*** (quantum interference, superposition etc.) that help us design Quantum Algorithms.
- To built intuition about the ***Quantum Computational model***.
- To understand what problems ***might*** benefit from a Quantum Computer.
- And which problems won't…

What this course is about

- To understand the nature of **Qbit**.
- To understand the principles of ***Quantum Mechanics*** (quantum interference, superposition etc.) that help us design Quantum Algorithms.
- To built intuition about the ***Quantum Computational model***.
- To understand what problems ***might*** benefit from a Quantum Computer.
- And which problems won't…
- Potential Applications.

What this course is about

And to convince you that Quantum theory and computing is not that difficult

And what is not about…

And what is not about…

- Quantum hardware.

And what is not about…

- Quantum hardware.
- The actual possibility of building a scalable Quantum Computer.

And what is not about…

- Quantum hardware.
- The actual possibility of building a scalable Quantum Computer.
- Quantum programming languages and simulations.

And what is not about…

- Quantum hardware.
- The actual possibility of building a scalable Quantum Computer.
- Quantum programming languages and simulations.
- Quantum Supremacy.

And what is not about…

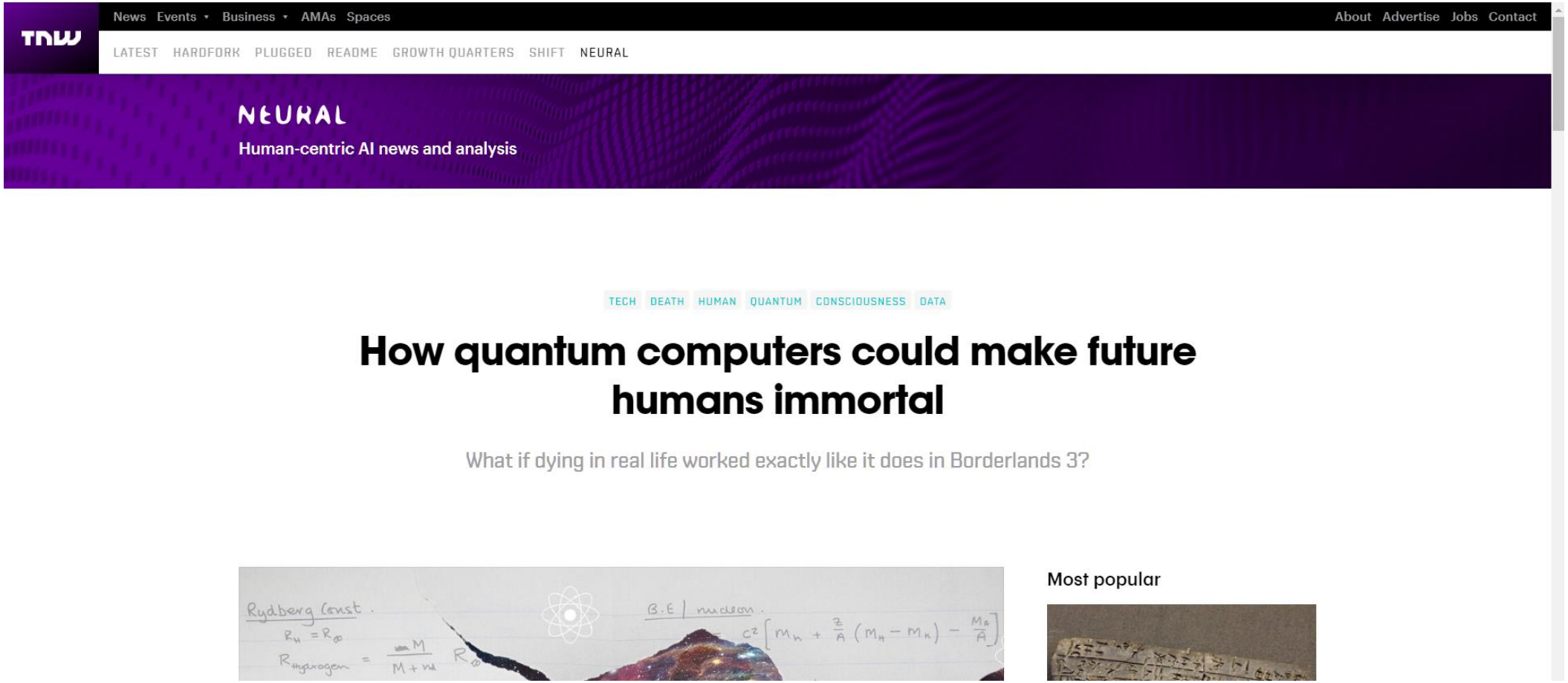
- Quantum hardware.
- The actual possibility of building a scalable Quantum Computer.
- Quantum programming languages and simulations.
- Quantum Supremacy.
- Any other “fancy” popular science thing related to QC.

And what is not about…

- Quantum hardware.
- The actual possibility of building a scalable Quantum Computer.
- Quantum programming languages and simulations.
- Quantum Supremacy.
- Any other “fancy” popular science thing related to QC.
- Philosophy.

What fancy things?

What fancy things?



What fancy things?

Home
Trending
Subscriptions
Library
History
Your videos

FILTER

Quantum Supremacy & AI, with Stephen Fry.
527K views • 11 months ago

Pindex

How **Quantum** AI could help you live to 200, like a bowhead whale. Google's **quantum** supremacy news opens exciting doors.

What is Quantum Computing?

What is Quantum Computing?

- To answer this, we first recall what is “**Computing**” in the classical sense.

What is Quantum Computing?

- To answer this, we first recall what is "**Computing**" in the classical sense.
- **Church-Turing Thesis**: anything that is computable, can be computed by an appropriate **Turing Machine**.

What is Quantum Computing?

- To answer this, we first recall what is "**Computing**" in the classical sense.
- **Church-Turing Thesis**: anything that is computable, can be computed by an appropriate **Turing Machine**.
- **Strong Church-Turing Thesis**: anything that can be ***efficiently*** computed in one model of computation, it can also be ***efficiently*** computed by an appropriate Turing Machine.

What is Quantum Computing?

- To answer this, we first recall what is "**Computing**" in the classical sense.
- **Church-Turing Thesis**: anything that is computable, can be computed by an appropriate **Turing Machine**.
- **Strong Church-Turing Thesis**: anything that can be ***efficiently*** computed in one model of computation, it can also be ***efficiently*** computed by an appropriate Turing Machine.

Efficient algorithm design is *independent* of underlying model of computation.

QC - Motivation

Classical computing (based on TM model of computation) does not seem able to efficiently simulate ***Quantum Mechanics***.

QC - Motivation

Classical computing (based on TM model of computation) does not seem able to efficiently simulate ***Quantum Mechanics***.

Deutsch: Can we justify Church-Turing thesis using laws of physics?

QC-Motivation

- New candidate universal machine: **Quantum machine**

QC-Motivation

- New candidate universal machine: **Quantum machine**
- Harnessing the power of nature (Quantum Mechanics)

QC-Motivation

- New candidate universal machine: **Quantum machine**
- Harnessing the power of nature (Quantum Mechanics)
- Is it possible that machines exploiting quantum structures can not be efficiently simulated on a Turing machine?

QC-Motivation

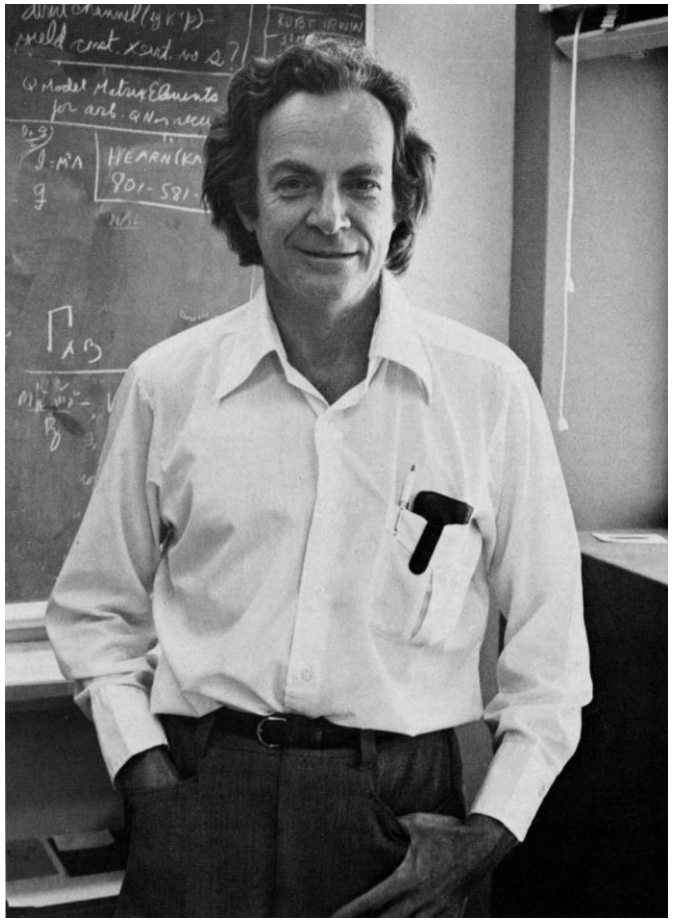
- New candidate universal machine: **Quantum machine**
- Harnessing the power of nature (Quantum Mechanics)
- Is it possible that machines exploiting quantum structures can not be efficiently simulated on a Turing machine?
- Is it possible that such Quantum machines can solve some problems ***provably faster*** than our standard Turing machines?

QC-Motivation

- New candidate universal machine: **Quantum machine**
- Harnessing the power of nature (Quantum Mechanics)
- Is it possible that machines exploiting quantum structures can not be efficiently simulated on a Turing machine?
- Is it possible that such Quantum machines can solve some problems ***provably faster*** than our standard Turing machines?

Violation of strong Church-Turing Thesis!

So…what is QC?



. . . trying to find a computer simulation of physics seems to me to be an excellent program to follow out. . . . the real use of it would be with quantum mechanics. . . . Nature isn't classical , dammit. . . and if you want to make a simulation of Nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.

Richard Feynman

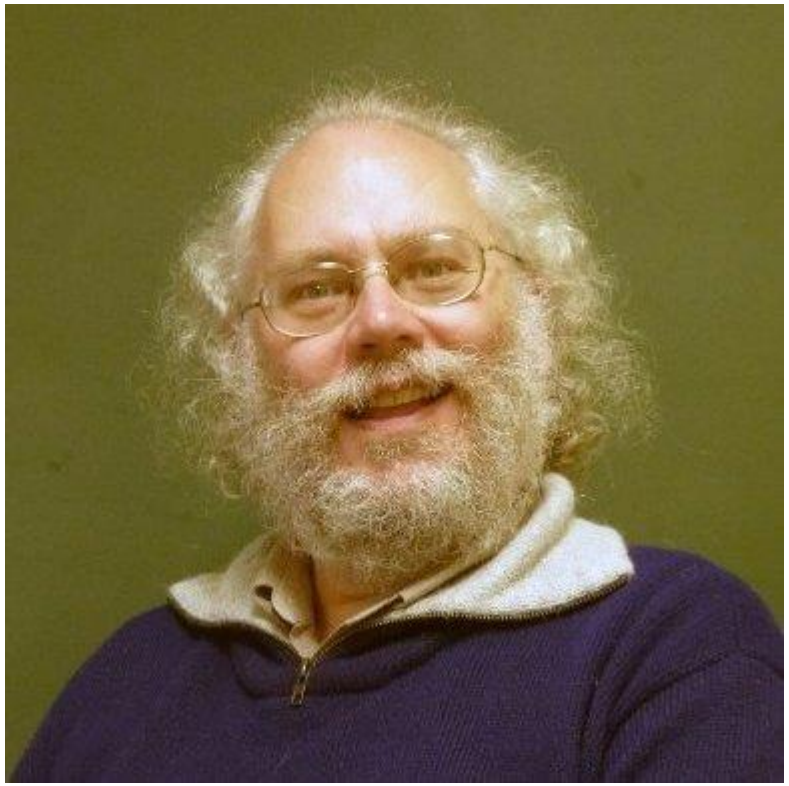
So…what is QC?

The theory of computation has traditionally been studied almost entirely in the abstract, as a topic in pure mathematics. This is to miss the point of it. Computers are physical objects, and computations are physical processes.
What computers can or cannot compute is determined by the laws of physics alone, and not by pure mathematics.

David Deutsch

But not much happened till…

But not much happened till…1994



But not much happened till…1994

- Peter Shor.

But not much happened till…1994

- Peter Shor.
- Described a ***fast purely Quantum Algorithm*** that can factor any positive integer into its prime components.

But not much happened till…1994

- Peter Shor.
- Described a ***fast purely Quantum Algorithm*** that can factor any positive integer into its prime components.
- We know how we can do it classically, but in ***exponential time.***

But not much happened till…1994

- Peter Shor.
- Described a ***fast purely Quantum Algorithm*** that can factor any positive integer into its prime components.
- We know how we can do it classically, but in ***exponential time.***
- The first algorithm that demonstrated that Quantum Computers can ***probably*** give an advantage over classical computation.

But not much happened till…1994

- Peter Shor.
- Described a ***fast purely Quantum Algorithm*** that can factor any positive integer into its prime components.
- We know how we can do it classically, but in ***exponential time.***
- The first algorithm that demonstrated that Quantum Computers can ***probably*** give an advantage over classical computation.
- Based on Quantum Fourier Transform.

But not much happened till…1994

- Peter Shor.
- Described a ***fast purely Quantum Algorithm*** that can factor any positive integer into its prime components.
- We know how we can do it classically, but in ***exponential time.***
- The first algorithm that demonstrated that Quantum Computers can ***probably*** give an advantage over classical computation.
- Based on Quantum Fourier Transform.
- Many applications (Cryptography, etc.)

But how does it perform in practice?

But how does it perform in practice?

- Shor’s Algorithm could factor 15 = 5 x 3 (2001) using 7 Qbits.

But how does it perform in practice?

- Shor’s Algorithm could factor 15 = 5 x 3 (2001) using 7 Qbits.
- Huge technological advancements led to factorization of 21 = 7 x 3

But how does it perform in practice?

- Shor's Algorithm could factor 15 = 5 x 3 (2001) using 7 Qbits.
- Huge technological advancements led to factorization of 21 = 7 x 3
- ***With high probability***

But how does it perform in practice?

- Shor's Algorithm could factor 15 = 5 x 3 (2001) using 7 Qbits.
- Huge technological advancements led to factorization of 21 = 7 x 3
- ***With high probability***
- *Maybe in the next decade we can factor 45 = 3 x 3 x 5!*

But how does it perform in practice?

- Shor's Algorithm could factor 15 = 5 x 3 (2001) using 7 Qbits.
- Huge technological advancements led to factorization of 21 = 7 x 3
- ***With high probability***
- *Maybe in the next decade we can factor 45 = 3 x 3 x 5!*

But how can we do that?

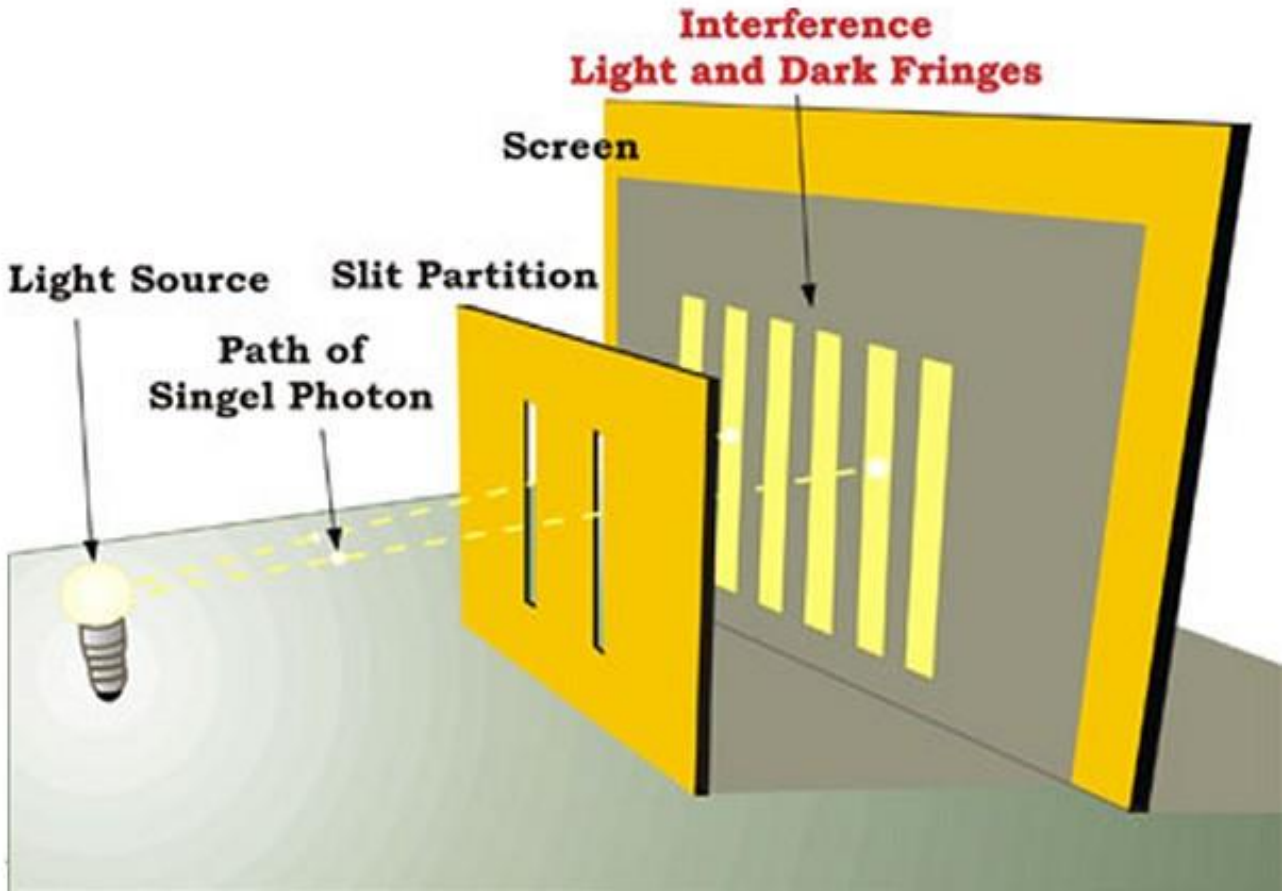
But how can we do that?

- We will describe two classical physics experiments that will give us insight about the quantum computational process

But how can we do that?

- We will describe two classical physics experiments that will give us insight about the quantum computational process
- And the nature of the new basic “carrier” of information (**Qbit**)

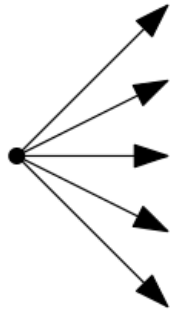
A bit of Physics: The Double Slit Experiment



- Source: https://www.physicsoftheuniverse.com/

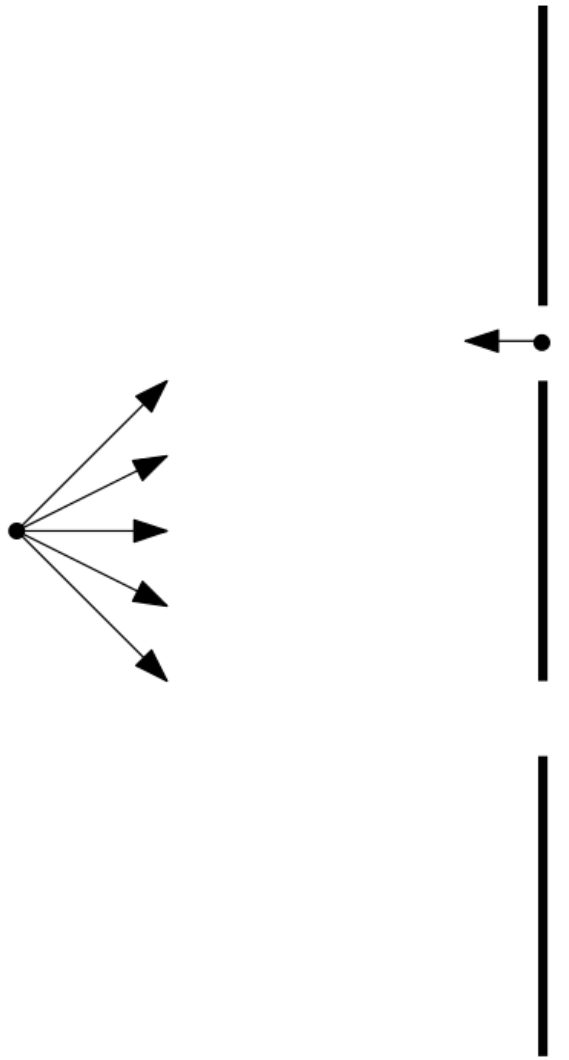
A bit of Physics: The Double Slit Experiment

- Beam of electrons



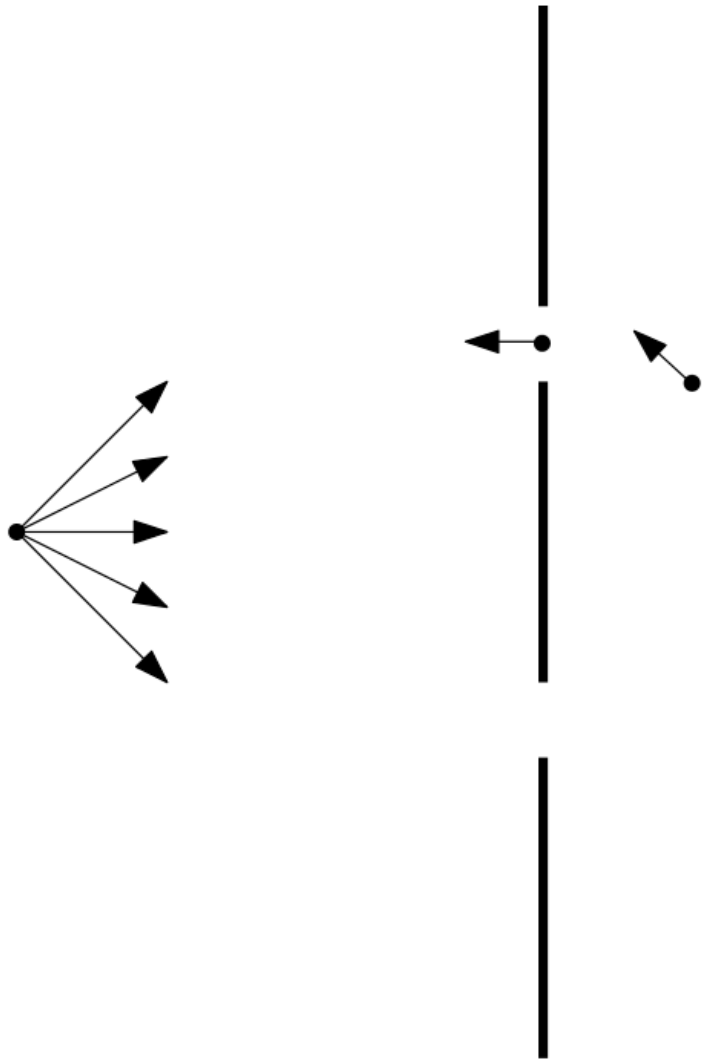
A bit of Physics: The Double Slit Experiment

- Beam of electrons



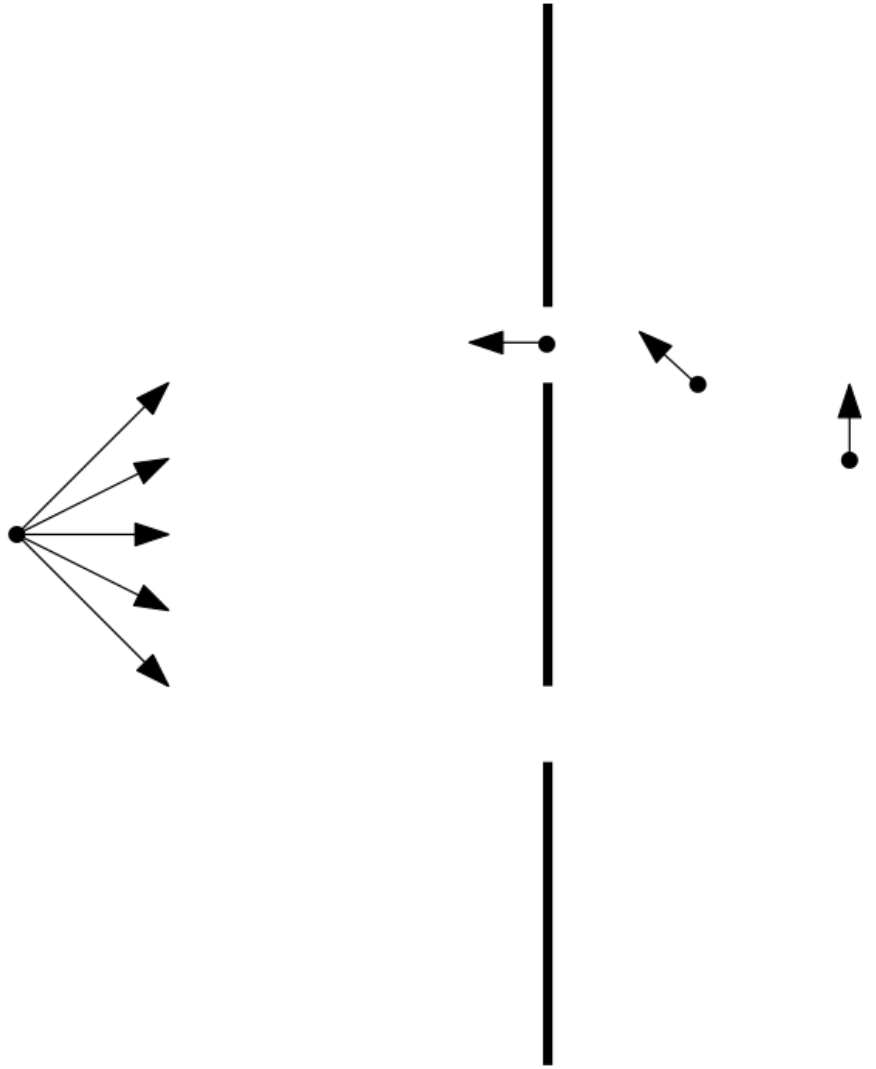
A bit of Physics: The Double Slit Experiment

- Beam of electrons



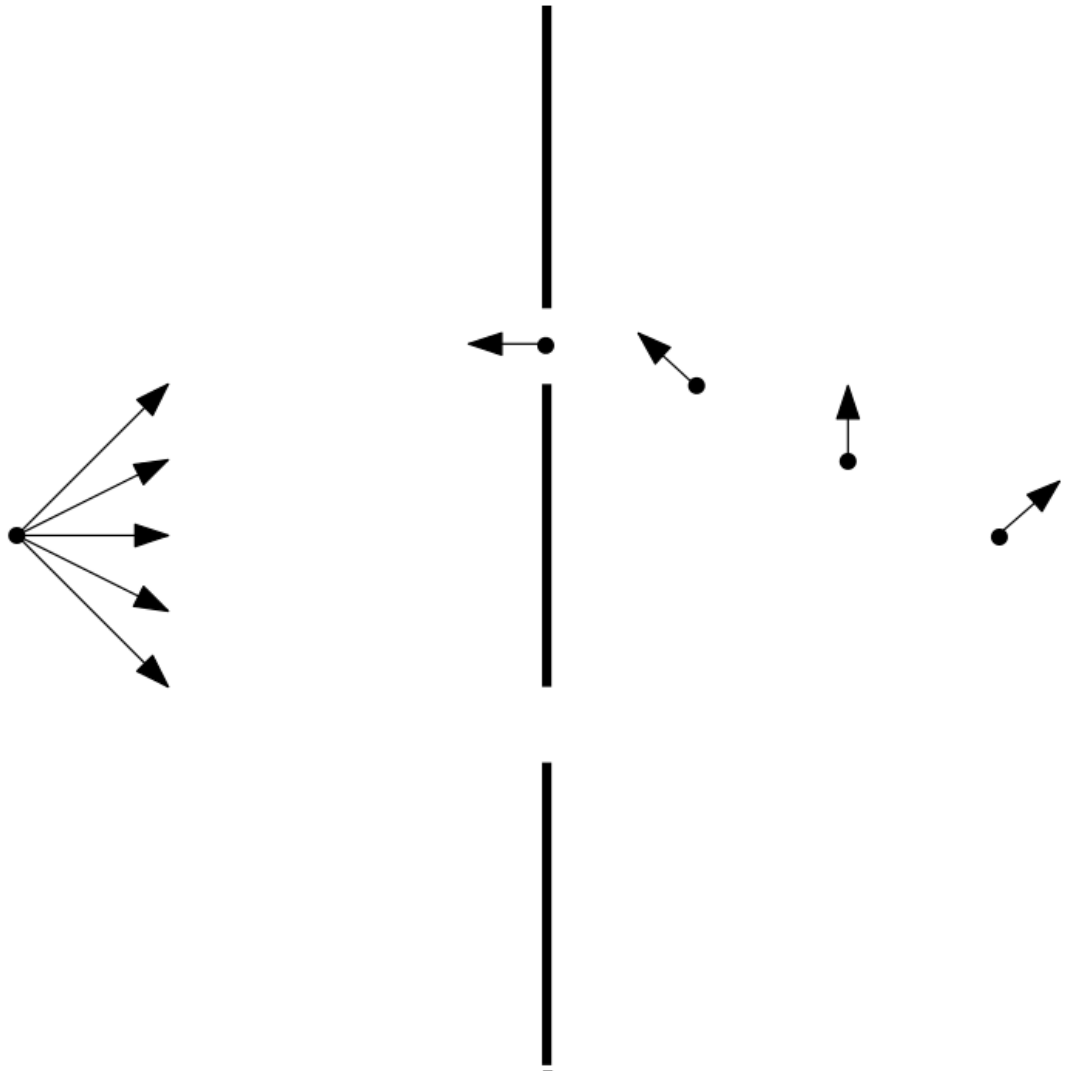
A bit of Physics: The Double Slit Experiment

- Beam of electrons



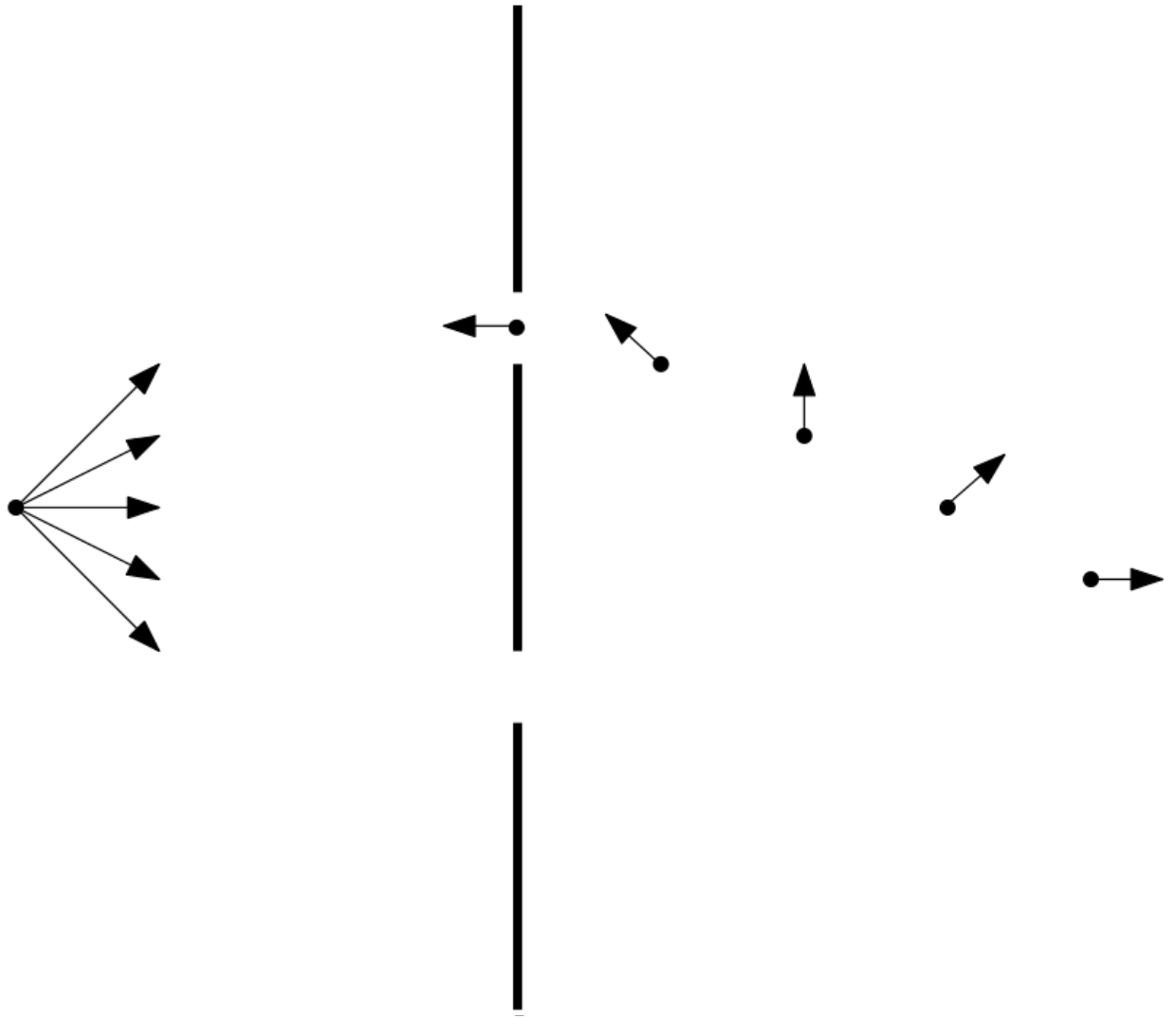
A bit of Physics: The Double Slit Experiment

- Beam of electrons



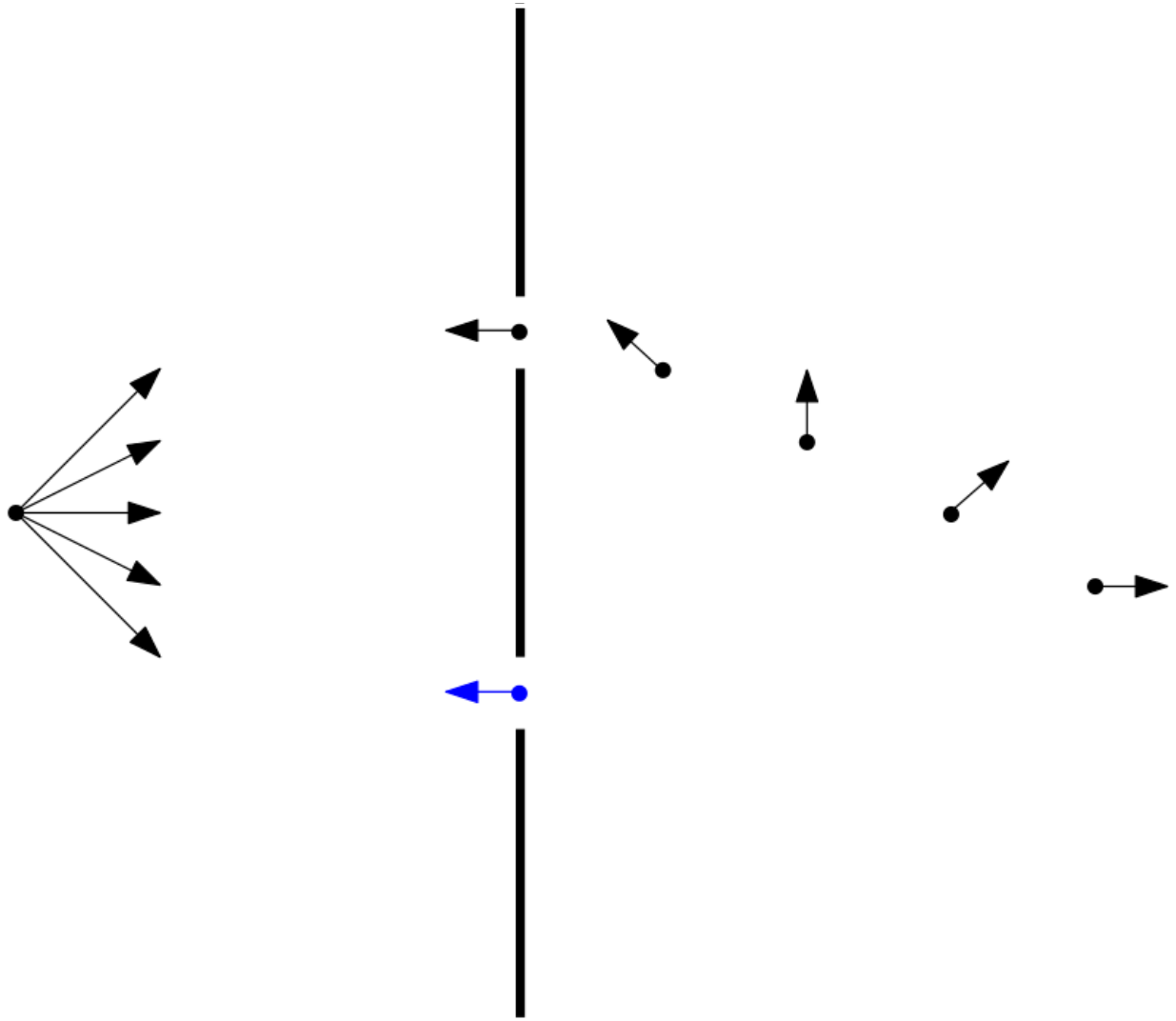
A bit of Physics: The Double Slit Experiment

- Beam of electrons



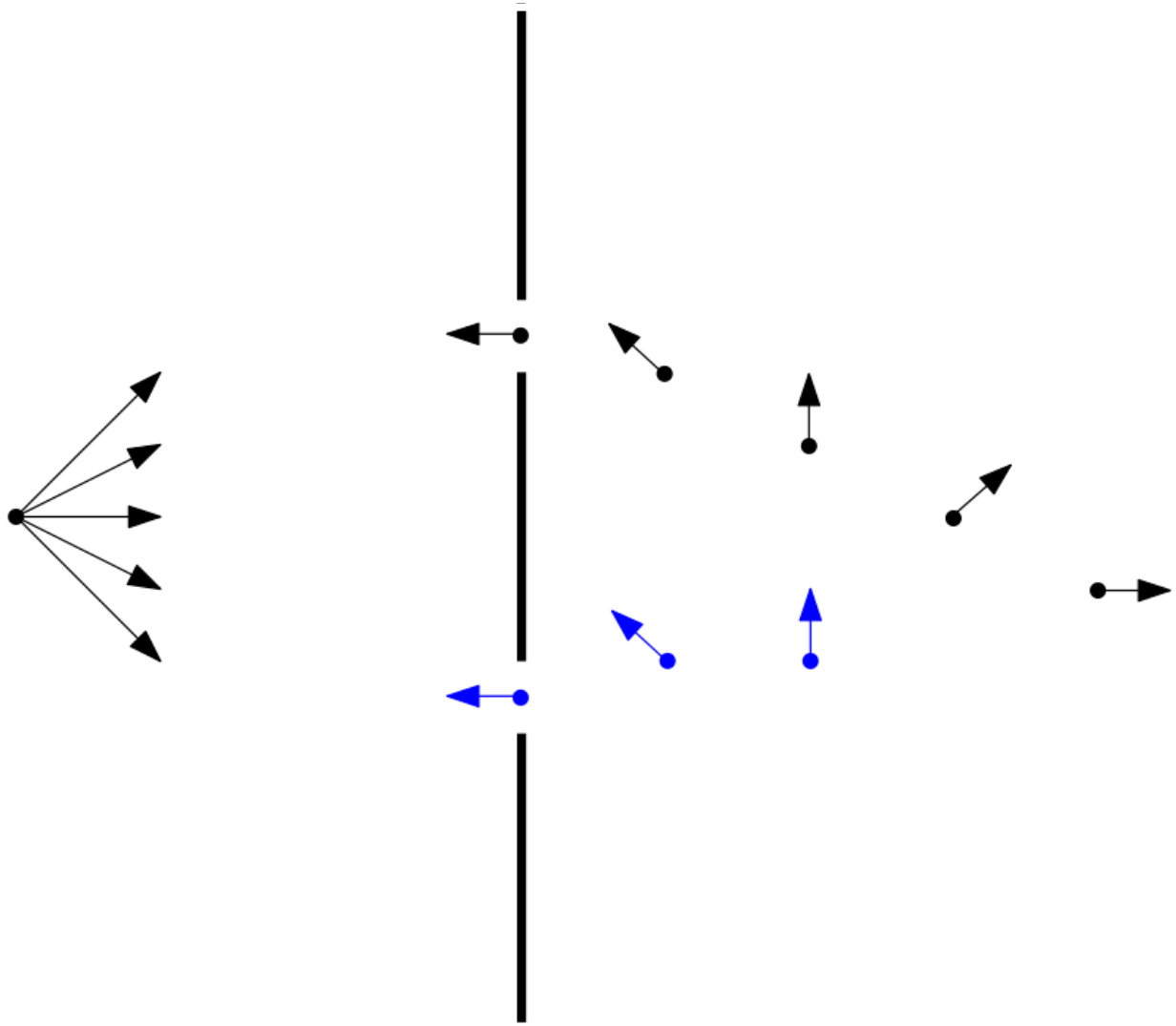
A bit of Physics: The Double Slit Experiment

- Beam of electrons



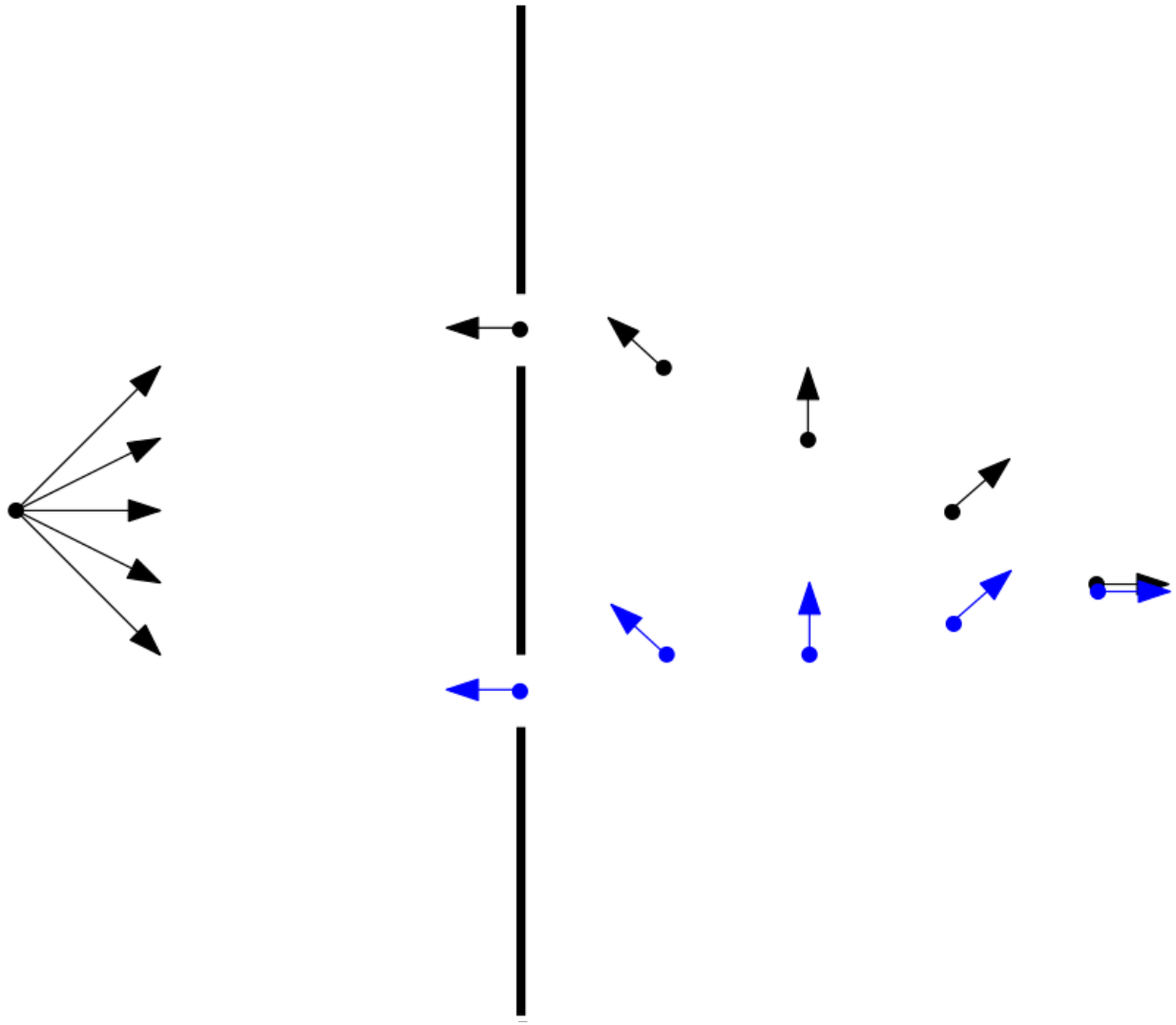
A bit of Physics: The Double Slit Experiment

- Beam of electrons



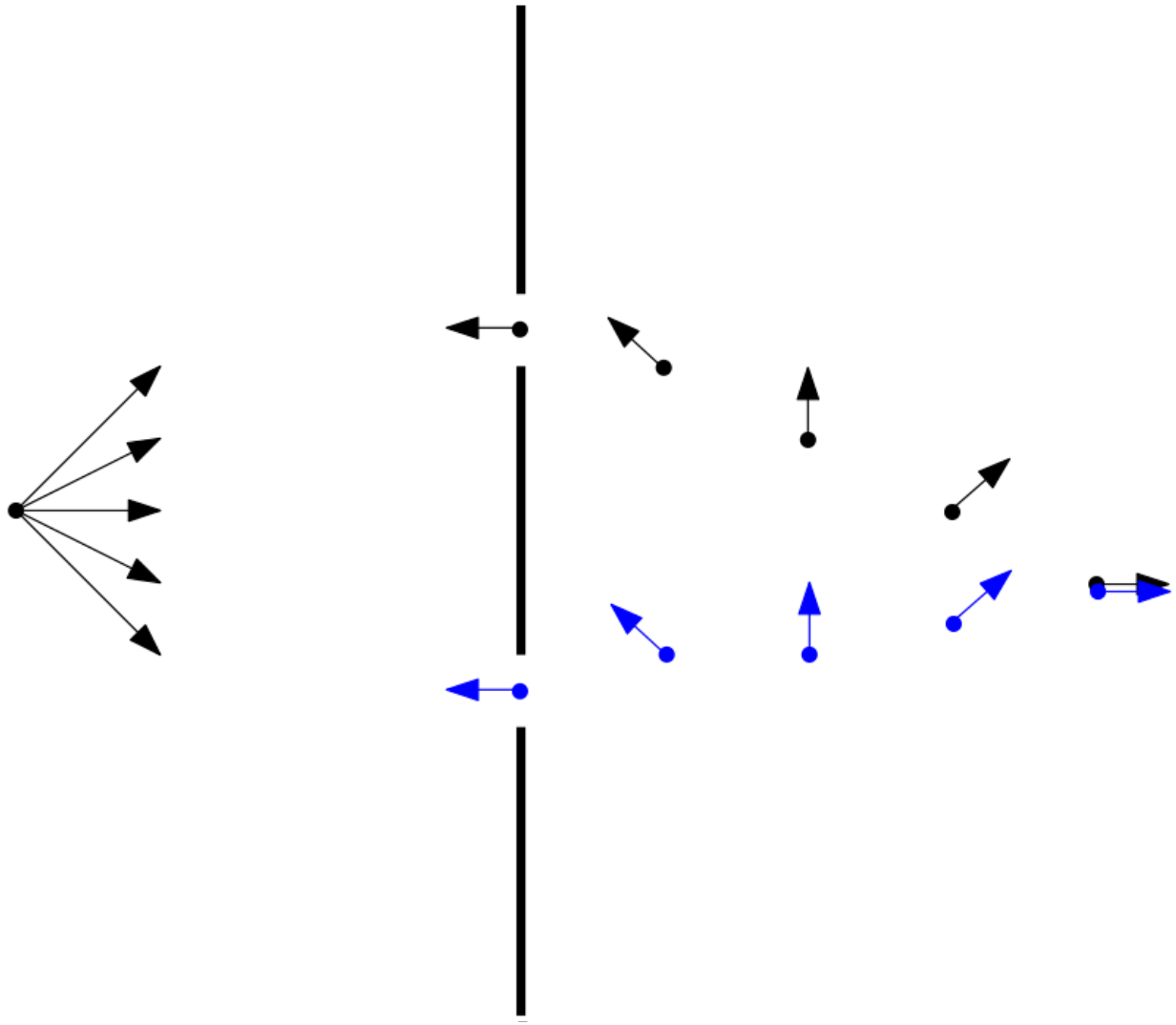
A bit of Physics: The Double Slit Experiment

- Beam of electrons



A bit of Physics: The Double Slit Experiment

- Beam of electrons

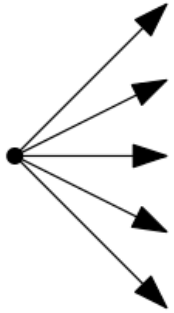


- ***Constructive***

Interference!

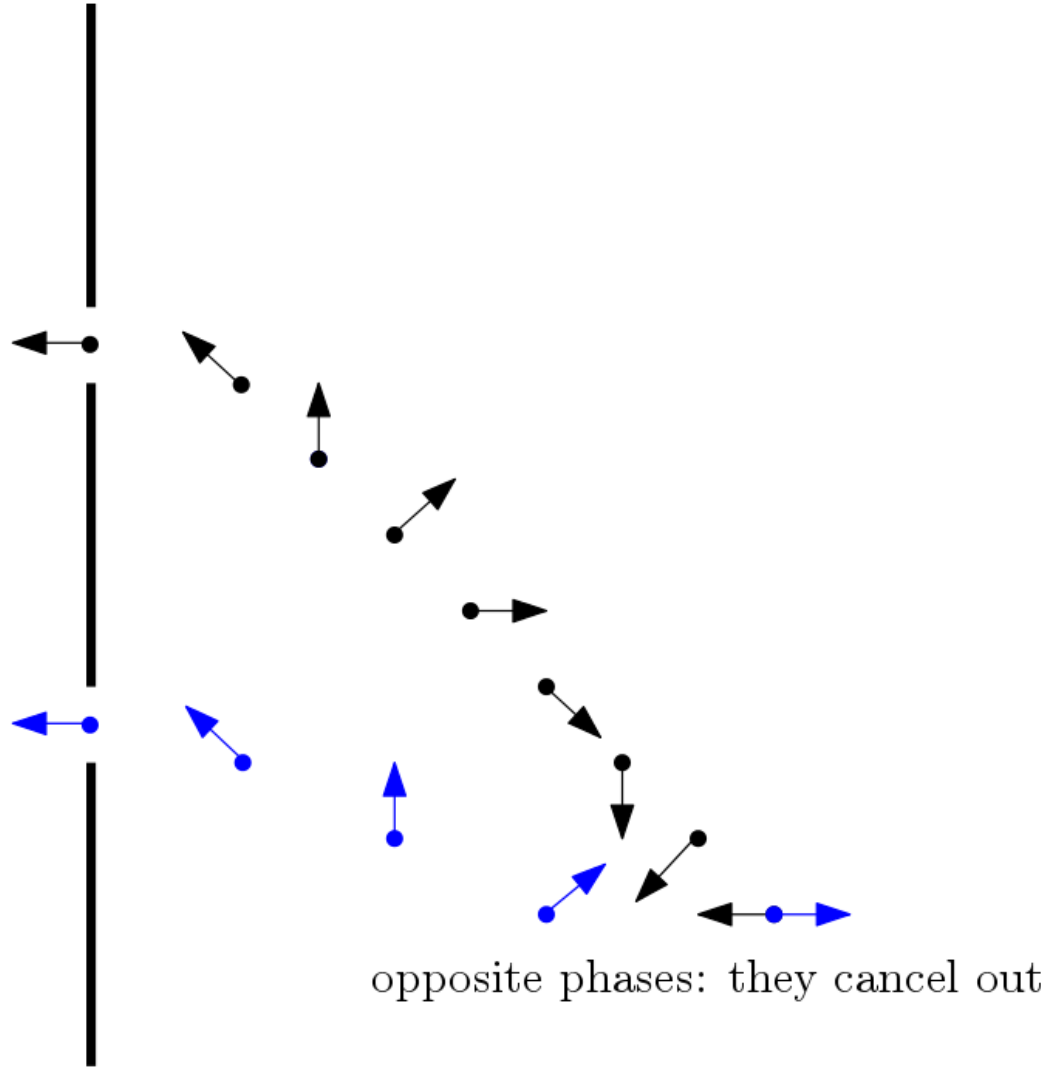
A bit of Physics: The Double Slit Experiment

- Beam of electrons



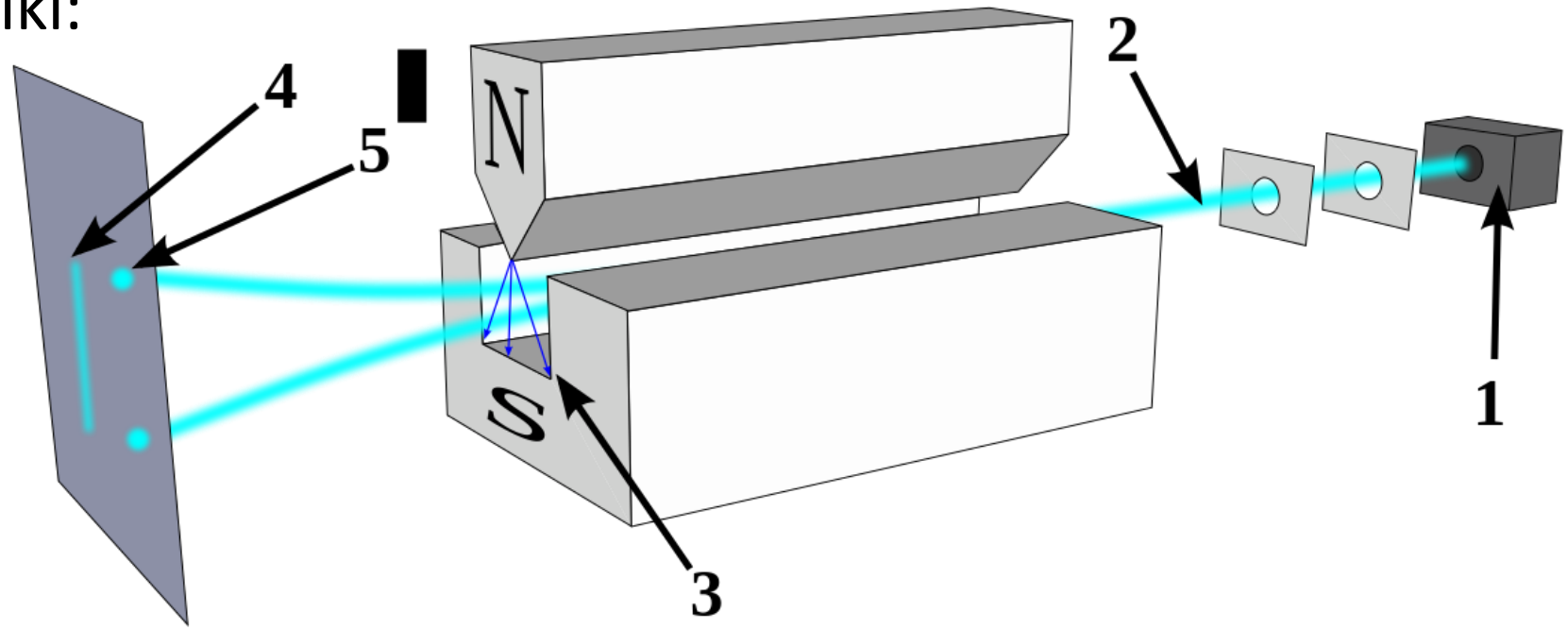
- ***Destructive***

Interference!



The Stern-Gerlach Experiment

- From wiki:



The Stern-Gerlach Experiment

- The “spin” is measured either up or down.

The Stern-Gerlach Experiment

- The “spin” is measured either up or down.
- No “in-between” values as predicted by classical physics.

The Stern-Gerlach Experiment

- The “spin” is measured either up or down.
- No “in-between” values as predicted by classical physics.
- If we keep measuring the orientation of all “up” spins, we will find that they are always oriented up.

The Stern-Gerlach Experiment

- The “spin” is measured either up or down.
- No “in-between” values as predicted by classical physics.
- If we keep measuring the orientation of all “up” spins, we will find that they are always oriented up.
- If we rotate the apparatus by 90 degrees and measure all previously “up” spins, then 50% of them are deflected to one direction and 50% on the other direction!

The Stern-Gerlach Experiment

- The “spin” is measured either up or down.
- No “in-between” values as predicted by classical physics.
- If we keep measuring the orientation of all “up” spins, we will find that they are always oriented up.
- If we rotate the apparatus by 90 degrees and measure all previously “up” spins, then 50% of them are deflected to one direction and 50% on the other direction!
- Classical physics say that none of them should be deflected at all!

The Quantum Bit: Qbit

The Quantum Bit: Qbit

- The elementary unit of quantum information.

The Quantum Bit: Qbit

- The elementary unit of quantum information.
- The quantum version of the classical ***bit:*** this can take values either **0 (false)** or **1 (true)**.
- Physical realizations of Qbit:

The Quantum Bit: Qbit

- The elementary unit of quantum information.
- The quantum version of the classical ***bit:*** this can take values either **0 (false)** or **1 (true)**.
- Physical realizations of Qbit:
  - Electron spin (Stern-Gerlach experiment): up (↑) or down (↓) spin.

The Quantum Bit: Qbit

- The elementary unit of quantum information.
- The quantum version of the classical ***bit:*** this can take values either **0 (false)** or **1 (true)**.
- Physical realizations of Qbit:
  - Electron spin (Stern-Gerlach experiment): up (↑) or down (↓) spin.
  - Polarization of a photon: vertical or horizontal polarization.

The Quantum Bit: Qbit

- The elementary unit of quantum information.
- The quantum version of the classical ***bit:*** this can take values either **0 (false)** or **1 (true)**.
- Physical realizations of Qbit:
  - Electron spin (Stern-Gerlach experiment): up (↑) or down (↓) spin.
  - Polarization of a photon: vertical or horizontal polarization.
- A classical bit (Cbit) can be either **0** or **1**.

The Quantum Bit: Qbit

- The elementary unit of quantum information.
- The quantum version of the classical ***bit:*** this can take values either **0 (false)** or **1 (true)**.
- Physical realizations of Qbit:
  - Electron spin (Stern-Gerlach experiment): up (↑) or down (↓) spin.
  - Polarization of a photon: vertical or horizontal polarization.
- A classical bit (Cbit) can be either **0** or **1**.
- A Qbit can also be in a ***coherent superposition of both***!

The Quantum Bit: Qbit

- When we look the value of a Cbit, its value remains **unchanged**.

The Quantum Bit: Qbit

- When we look the value of a Cbit, its value remains **unchanged**.
- When we look a value of a **Qbit** that is in superposition of two (or more) states, then its superposition ***collapses*** and the Qbit goes into exactly one of its states.

The Quantum Bit: Qbit

- When we look the value of a Cbit, its value remains **unchanged**.
- When we look a value of a **Qbit** that is in superposition of two (or more) states, then its superposition ***collapses*** and the Qbit goes into exactly one of its states.
- An electron spin s can be ↑ or ↓ or in a superposition of them

The Quantum Bit: Qbit

- When we look the value of a Cbit, its value remains **unchanged**.
- When we look a value of a **Qbit** that is in superposition of two (or more) states, then its superposition ***collapses*** and the Qbit goes into exactly one of its states.
- An electron spin s can be ↑ or ↓ or in a superposition of them

$$|\boldsymbol{s}\rangle = \boldsymbol{\alpha}\ |\uparrow\rangle + \boldsymbol{\beta}\ |\downarrow\rangle$$

The Quantum Bit: Qbit

- When we look the value of a Cbit, its value remains **unchanged**.
- When we look a value of a **Qbit** that is in superposition of two (or more) states, then its superposition ***collapses*** and the Qbit goes into exactly one of its states.
- An electron spin s can be ↑ or ↓ or in a superposition of them

$$|\boldsymbol{s}\rangle = \boldsymbol{\alpha}\ |\uparrow\rangle + \boldsymbol{\beta}\ |\downarrow\rangle$$

- Such that $\boldsymbol{\alpha^2 + \beta^2 = 1}$.

The Quantum Bit: Qbit

- When we look the value of a Cbit, its value remains **unchanged**.
- When we look a value of a **Qbit** that is in superposition of two (or more) states, then its superposition ***collapses*** and the Qbit goes into exactly one of its states.
- An electron spin s can be ↑ or ↓ or in a superposition of them

$$|\boldsymbol{s}\rangle = \boldsymbol{\alpha}\ |\uparrow\rangle + \boldsymbol{\beta}\ |\downarrow\rangle$$

- Such that $\boldsymbol{\alpha^2 + \beta^2 = 1}$.
- This intuitively means that if we observe s we will see ↑ spin with *probability* $\boldsymbol{\alpha^2}$ and ↓ spin with *probability* $\boldsymbol{\beta^2}$.

The Quantum Bit: Qbit

- The numbers α, β can be any numbers (reals, negative, complex).

The Quantum Bit: Qbit

- The numbers α, β can be any numbers (reals, negative, complex).
- They are called the ***amplitudes*** of the corresponding state.

The Quantum Bit: Qbit

- The numbers α, β can be any numbers (reals, negative, complex).
- They are called the ***amplitudes*** of the corresponding state.
- Then we don't we describe the quantum state as simply

$$|\boldsymbol{s}\rangle = \boldsymbol{\alpha^2}\ |\uparrow\rangle + \boldsymbol{\beta^2}\ |\downarrow\rangle?$$

The Quantum Bit: Qbit

- The numbers α, β can be any numbers (reals, negative, complex).
- They are called the ***amplitudes*** of the corresponding state.
- Then we don't we describe the quantum state as simply

$$|\boldsymbol{s}\rangle = \boldsymbol{\alpha^2}\ |\uparrow\rangle + \boldsymbol{\beta^2}\ |\downarrow\rangle?$$

- If we allow amplitudes to be negative, then we allow ***negative interference*** between different computational paths that lead to incorrect solutions!

The Quantum Bit: Qbit

- The numbers α, β can be any numbers (reals, negative, complex).
- They are called the ***amplitudes*** of the corresponding state.
- Then we don't we describe the quantum state as simply

$$|\boldsymbol{s}\rangle = \boldsymbol{\alpha^2}\ |\uparrow\rangle + \boldsymbol{\beta^2}\ |\downarrow\rangle?$$

- If we allow amplitudes to be negative, then we allow ***negative interference*** between different computational paths that lead to incorrect solutions!
- Such "forbidden" computational paths cancel out!

The Quantum Bit: Qbit

- The numbers α, β can be any numbers (reals, negative, complex).
- They are called the ***amplitudes*** of the corresponding state.
- Then we don't we describe the quantum state as simply

$$|\boldsymbol{s}\rangle = \boldsymbol{\alpha^2}\ |\uparrow\rangle + \boldsymbol{\beta^2}\ |\downarrow\rangle?$$

- If we allow amplitudes to be negative, then we allow ***negative interference*** between different computational paths that lead to incorrect solutions!
- Such "forbidden" computational paths cancel out!
- We cannot do that with a classical computer!

The Quantum Bit: Qbit

- Another reason why we like negative amplitudes: By allowing that, then we are greatly enhancing the set of operations that we can perform on a Qbit.

The Quantum Bit: Qbit

- Another reason why we like negative amplitudes: By allowing that, then we are greatly enhancing the set of operations that we can perform on a Qbit.
- These are the ***unitary operators*** (linear transformations that preserve the length of the vector).

The Quantum Bit: Qbit

- Another reason why we like negative amplitudes: By allowing that, then we are greatly enhancing the set of operations that we can perform on a Qbit.
- These are the ***unitary operators*** (linear transformations that preserve the length of the vector).
- Such transformations are in the core of every quantum algorithm.

The Quantum Bit: Qbit

- Another reason why we like negative amplitudes: By allowing that, then we are greatly enhancing the set of operations that we can perform on a Qbit.
- These are the ***unitary operators*** (linear transformations that preserve the length of the vector).
- Such transformations are in the core of every quantum algorithm.
- And why complex numbers?
- That’s much more complicated question but fortunately we won’t need them ☺

Qbits vs Cbits

Quantum bits are distinguished from Cbits by three phenomena:

Qbits vs Cbits

Quantum bits are distinguished from Cbits by three phenomena:

- *Superposition*

Qbits vs Cbits

Quantum bits are distinguished from Cbits by three phenomena:

- *Superposition*
- *Interference*

Qbits vs Cbits

Quantum bits are distinguished from Cbits by three phenomena:

- *Superposition*
- *Interference*
- *Entanglement*

Qbits vs Cbits

Quantum bits are distinguished from Cbits by three phenomena:

- *Superposition*
- *Interference*
- *Entanglement*
- One Qbit can encode ***up to two classical bits of information***.

Qbits vs Cbits

Quantum bits are distinguished from Cbits by three phenomena:

- *Superposition*
- *Interference*
- *Entanglement*
- One Qbit can encode ***up to two classical bits of information***.
- This is done via ***Super-dense coding***.

Qbits vs Cbits

Quantum bits are distinguished from Cbits by three phenomena:

- *Superposition*
- *Interference*
- *Entanglement*
- One Qbit can encode ***up to two classical bits of information***.
- This is done via ***Super-dense coding***.

These can be represented in information theoretical terms by a qubit, and the operations thereon, and throughout this course we will see how these phenomena give rise to powerful quantum algorithms.