CS 258: Quantum Cryptography

Mark Zhandry

Previously…

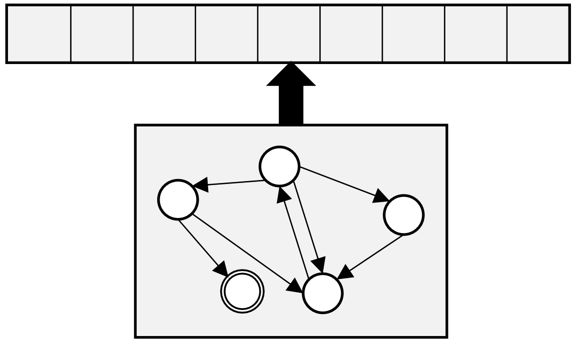
The Fundamental Formula of Modern Cryptography

Secure Cryptosystem = Protocol + Formal Security Model **M** + Computational Assumption **P** + Proof that **P** implies **M**

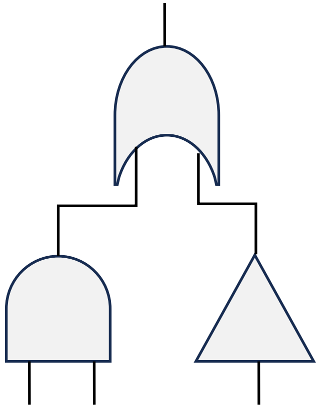
All of these deal with "efficient" adversaries

What is "efficient" computation?

1900's – Present: can run *efficiently* on *today's* computers



Turing machines

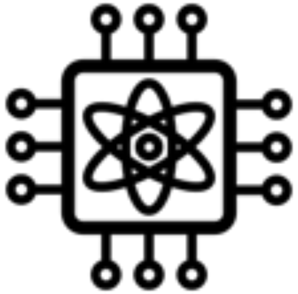


(Classical) circuits

(Extended) Church-Turing Thesis: Today's computers can (efficiently) compute anything that can be (efficiently) computed by *any* physical process

What is "efficient" computation?

The future: can run *efficiently* on *quantum* computers



(Extended) Church-Turing Thesis: Today's computers can (efficiently) compute anything that can be (efficiently) computed by *any* physical process

Today: Introduction to Quantum Mechanics

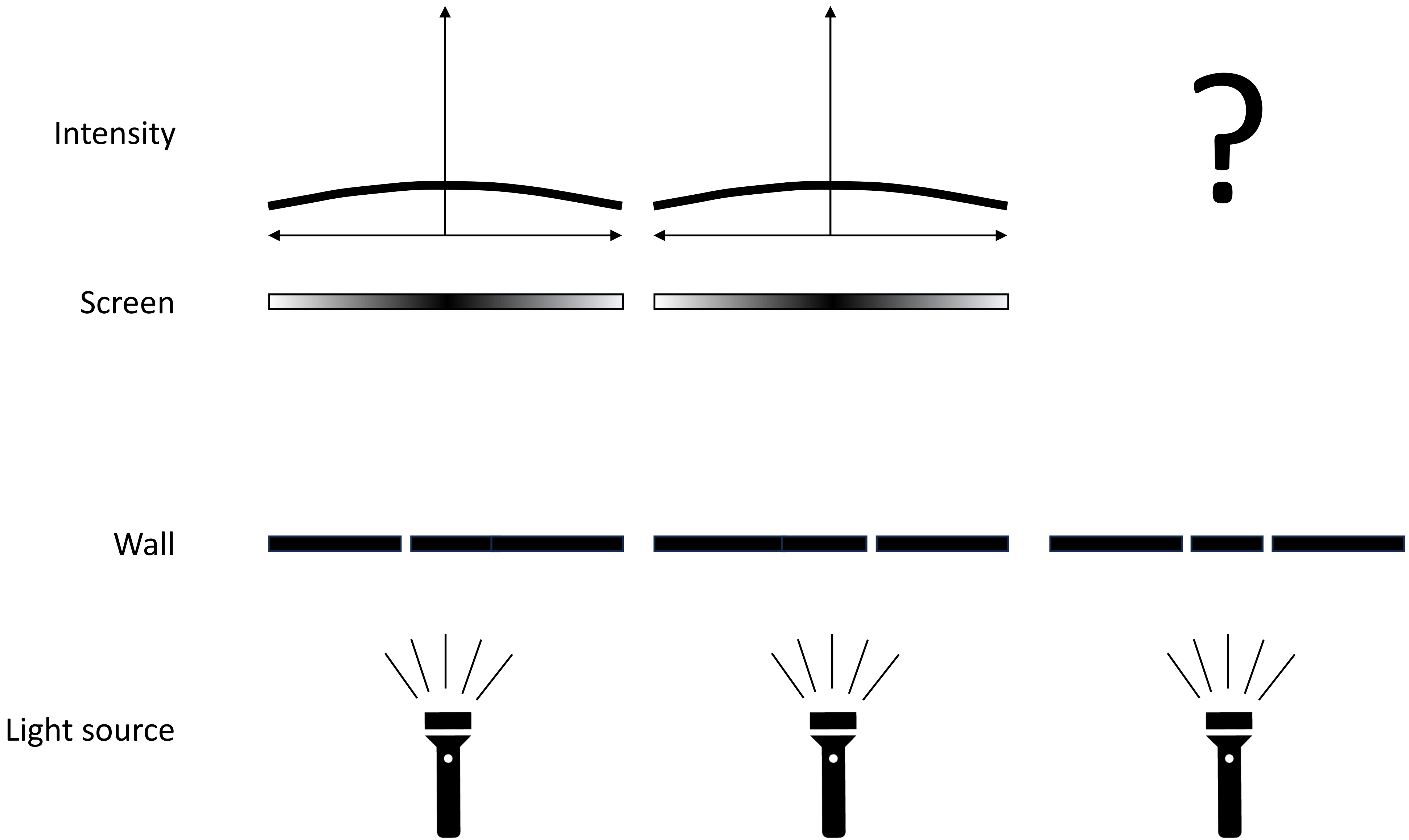
Fundamental Q:

Dates back to 1600s

Is light made of particles or waves?

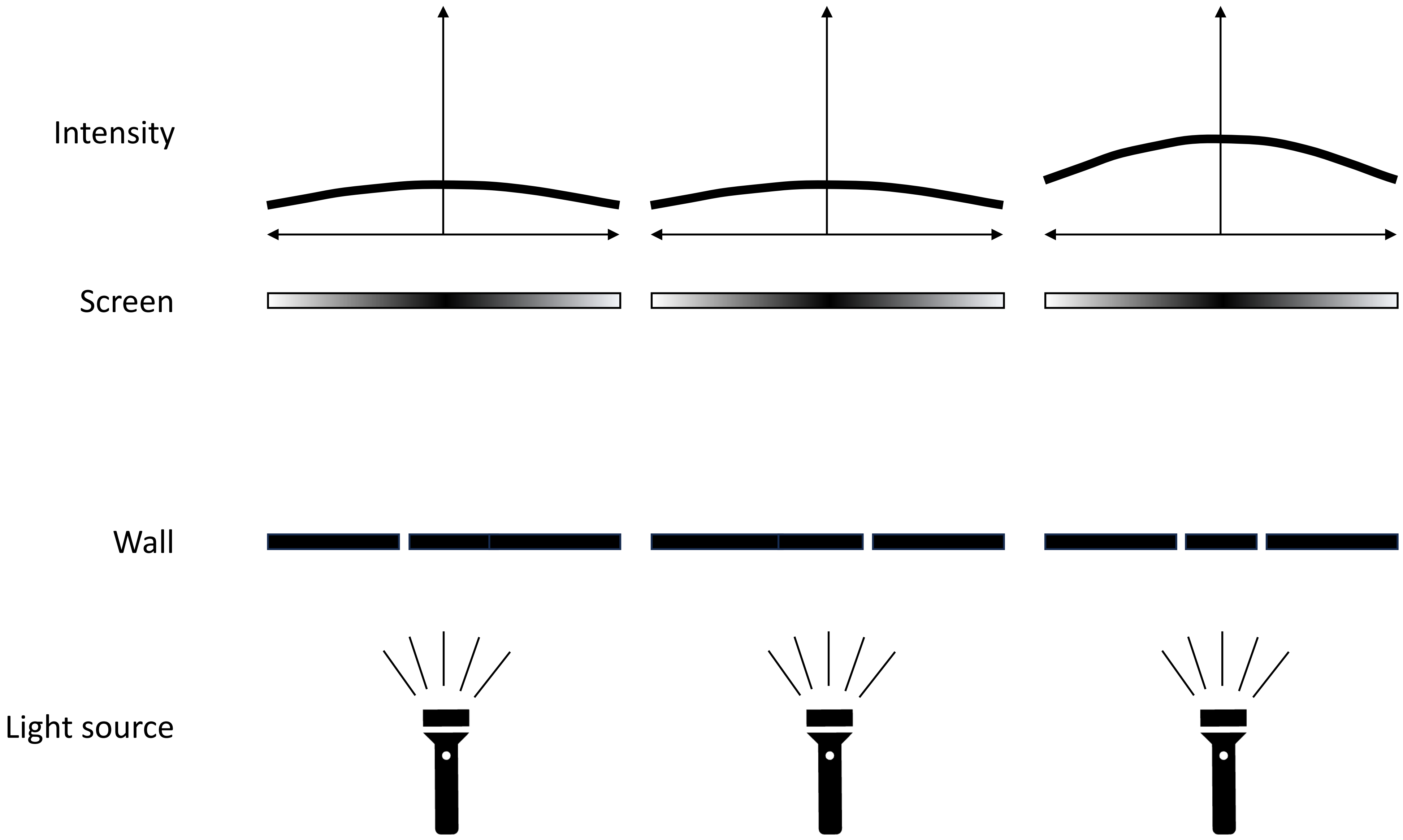
Evidence for particle theory or light: Young’s double slit experiment

(1801)

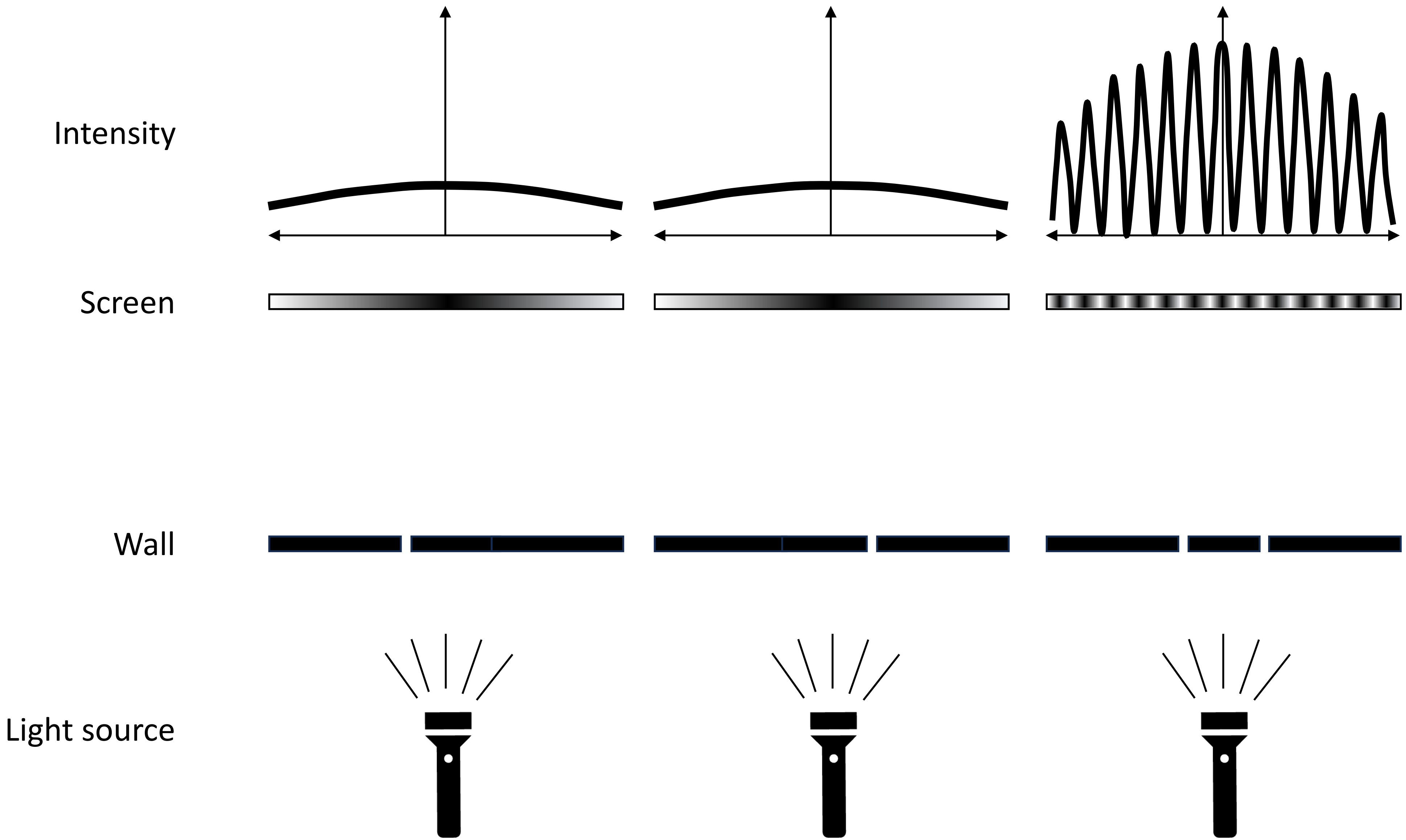


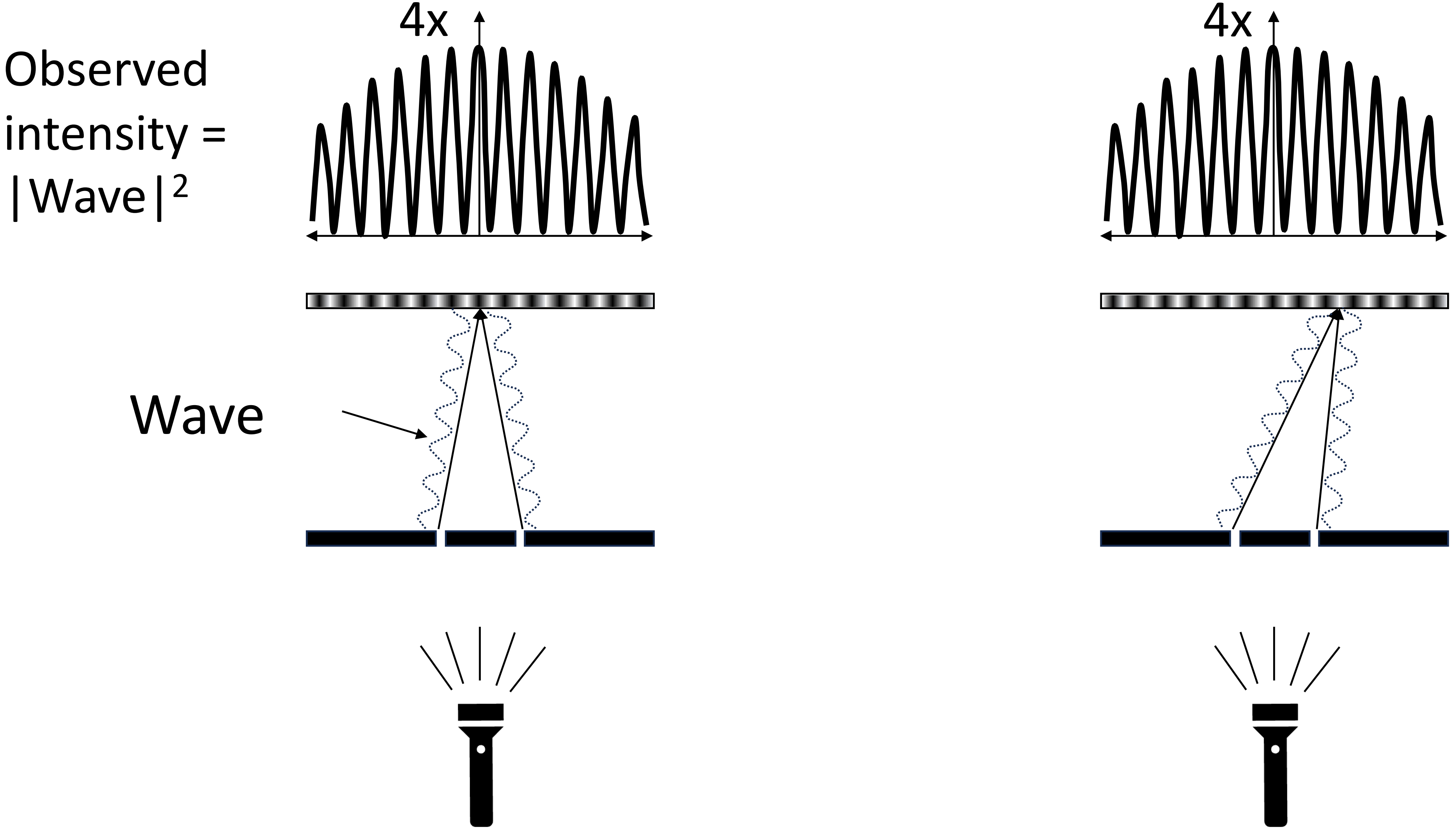
Intensity
Screen
Wall
Light source
?

Prediction from **particle** theory of light:



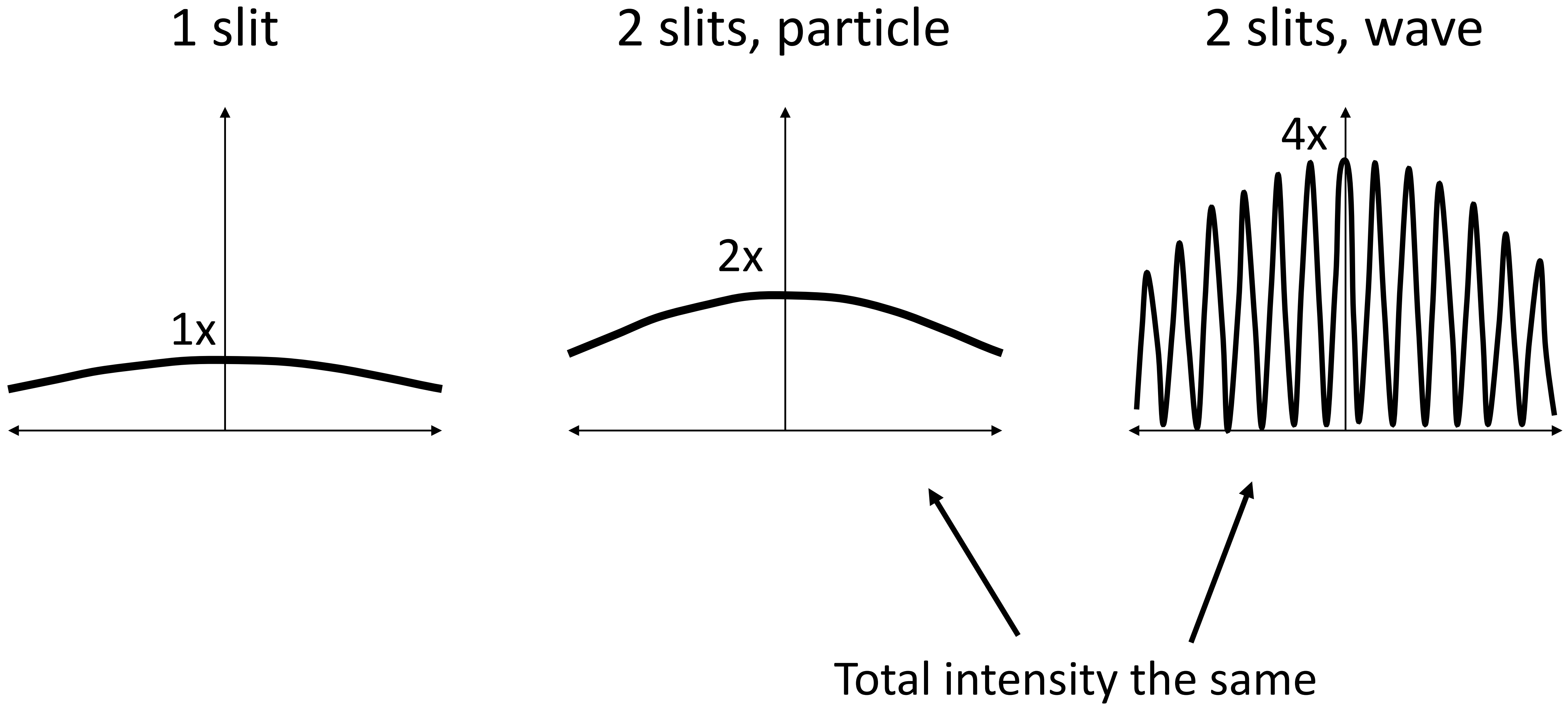
Prediction from **wave** theory of light:



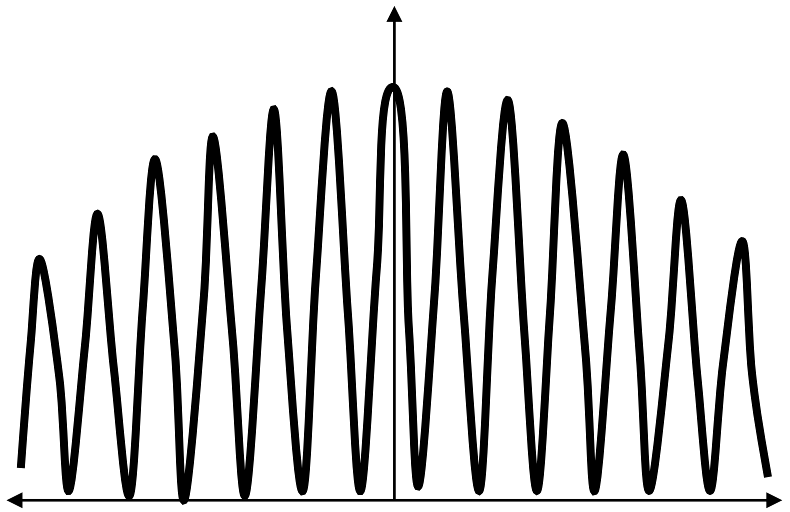


Constructive Interference

Destructive Interference


1 slit
2 slits, particle
2 slits, wave
1x
2x
4x
Total intensity the same

Outcome of Young's double slit experiment:

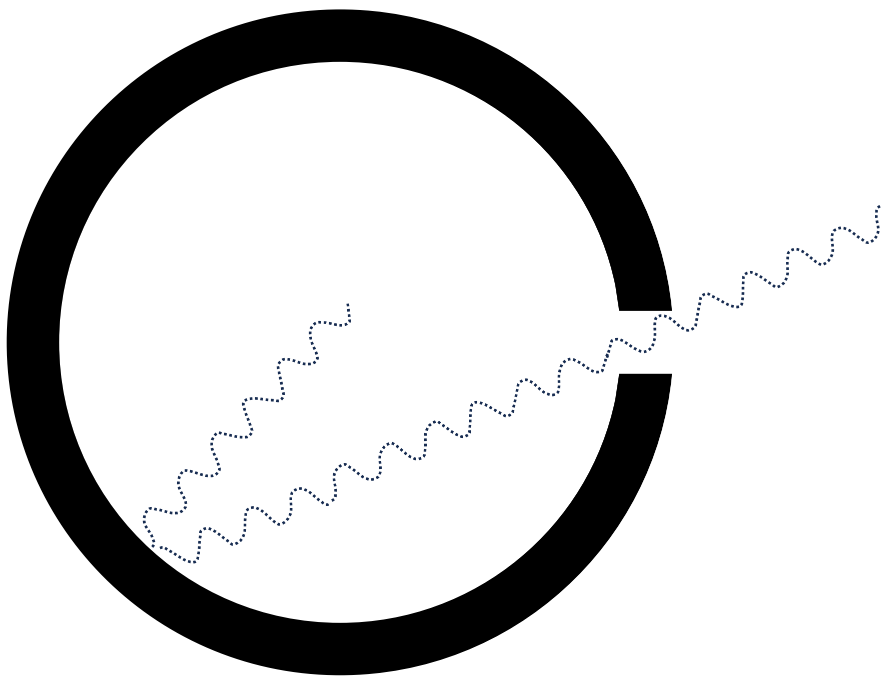


Therefore, light must be a wave!

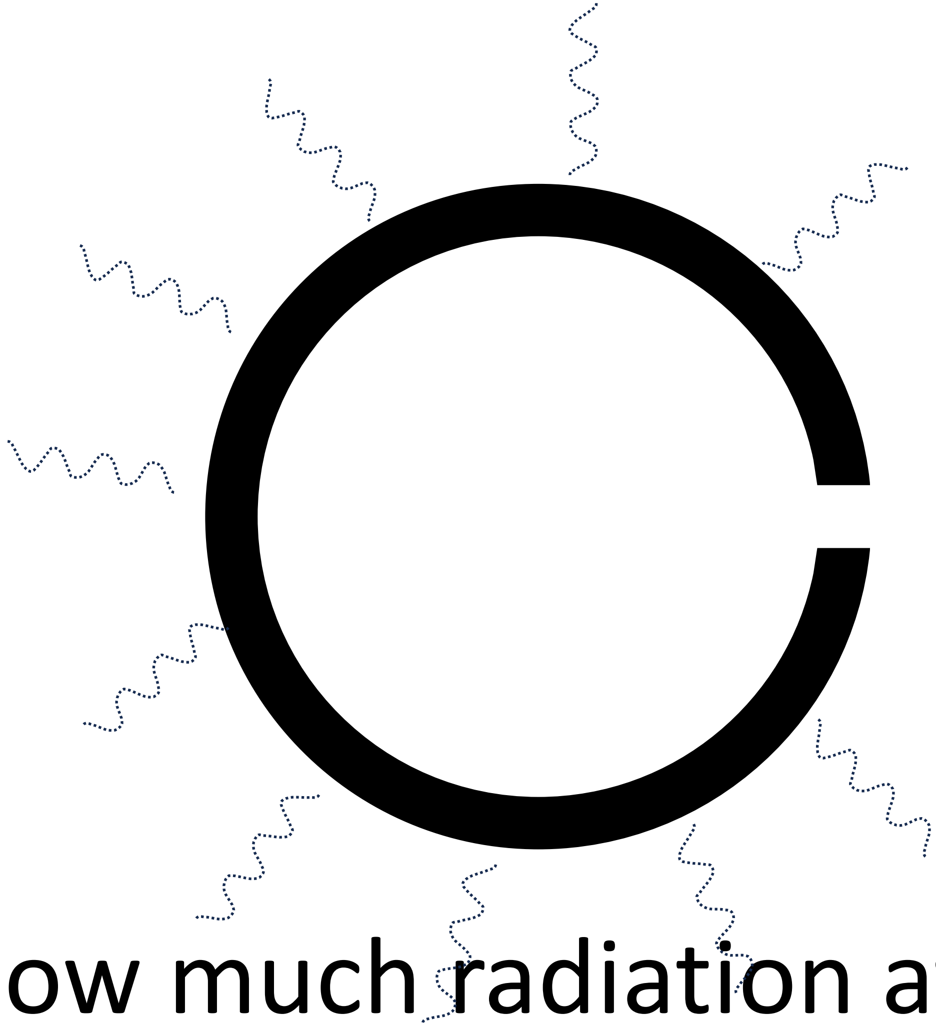
Evidence for particle theory or light: The ultraviolet catastrophe

(1900’s)

Ideal black body = absorb all incoming light

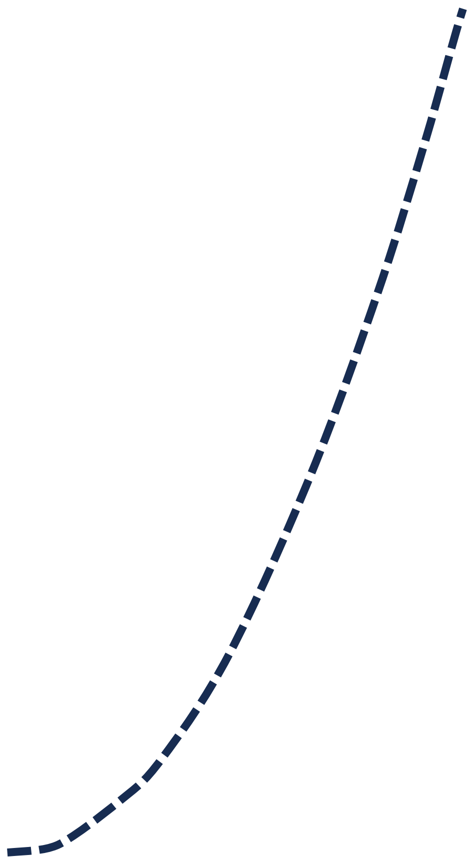


Classical thermodynamics: ideal black bodies emit radiation (light)



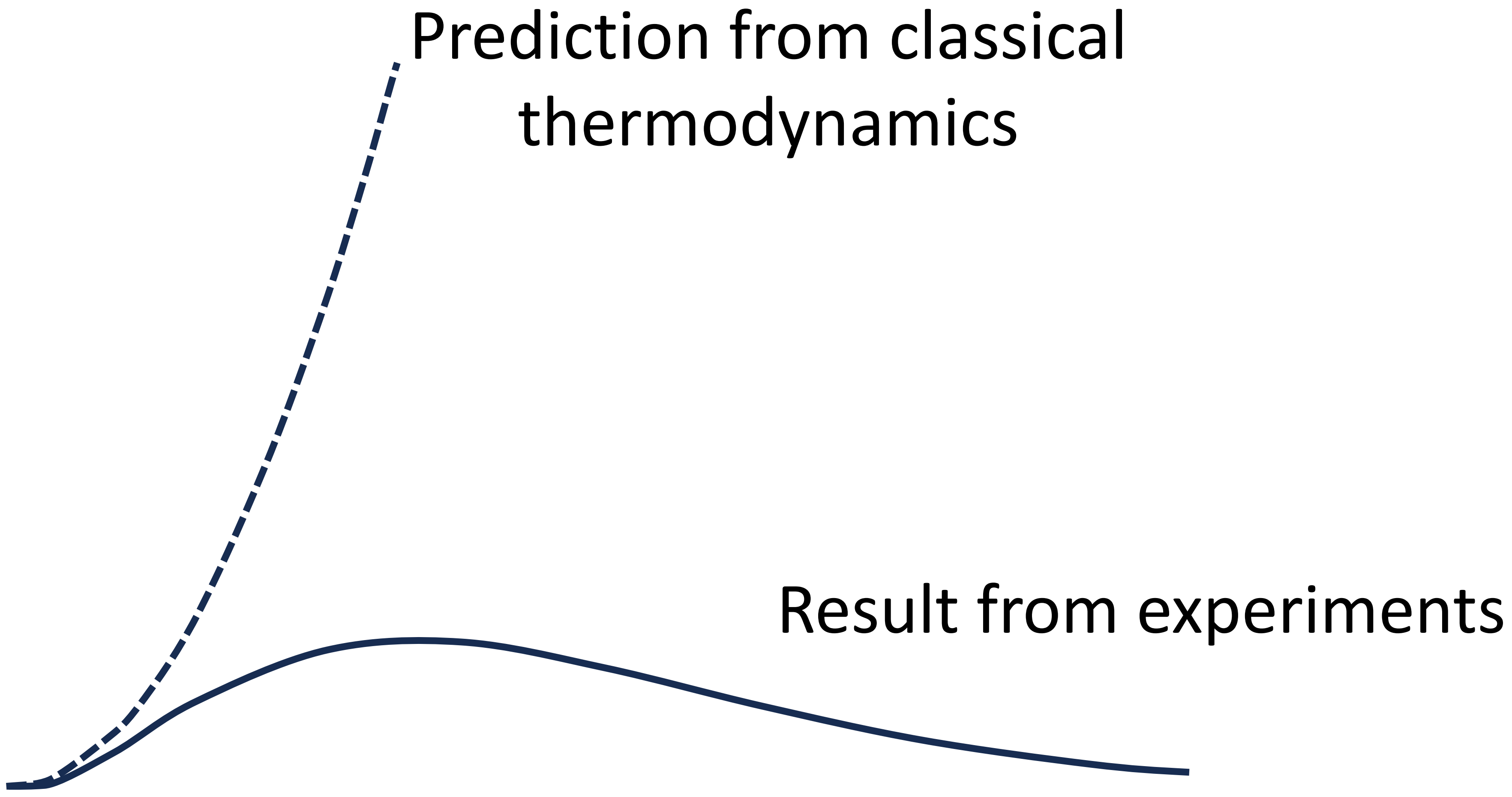
Also predict how much radiation at each frequency

The Ultraviolet Catastrophe



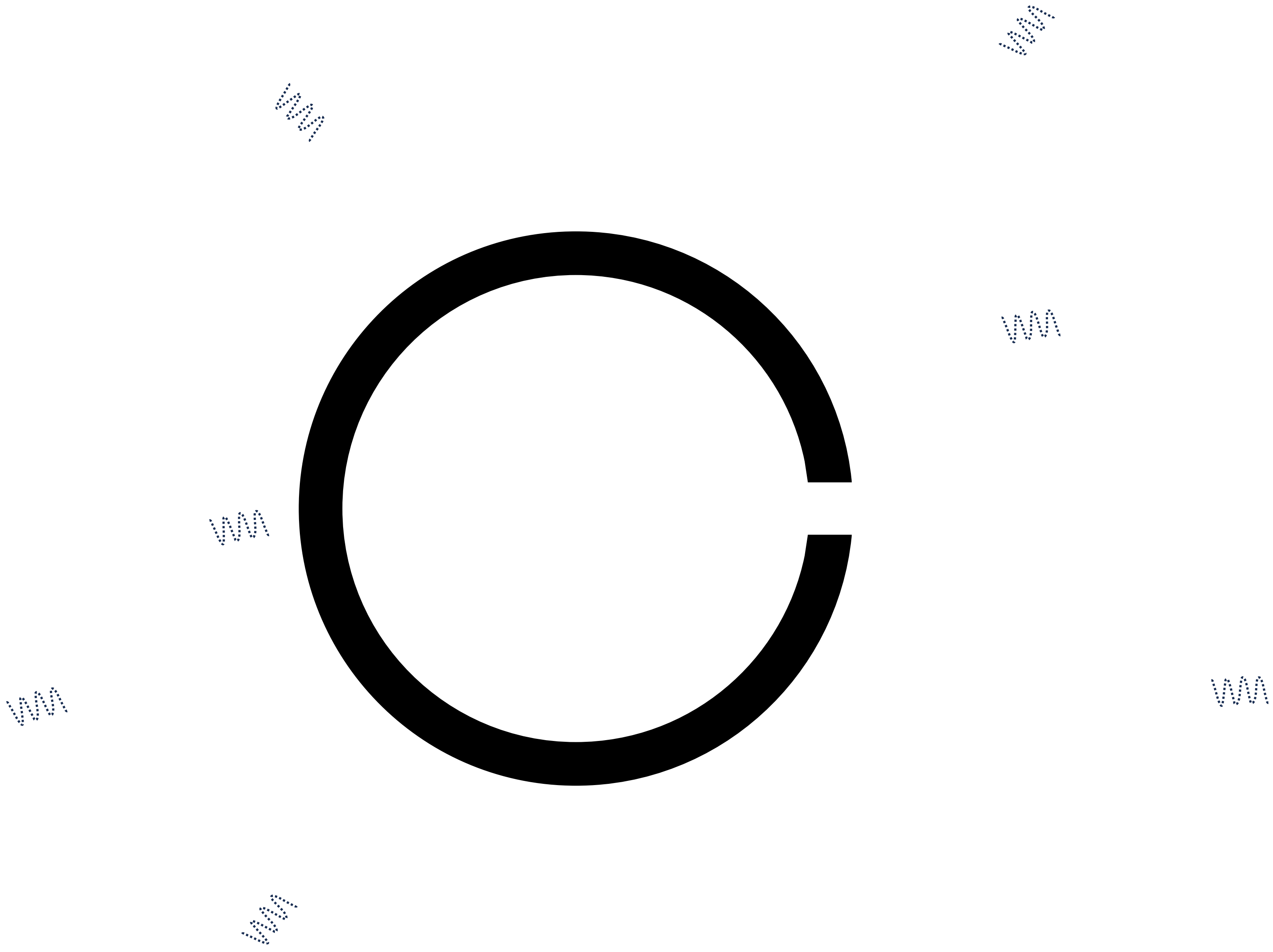
Prediction from classical thermodynamics

Obvious problem: total radiation is infinite!


Prediction from classical thermodynamics
Result from experiments

Solution: Quantize Light

Plank, 1900



Solution: Quantize Light

Plank, 1900

Prediction using quantized light
exactly matches experiments

Initially, quantizing light was proposed just as a way to get the math to work out

Einstein (1905) proposed that quantized light was actually physical (now called photons); used it to explain the photoelectric effect

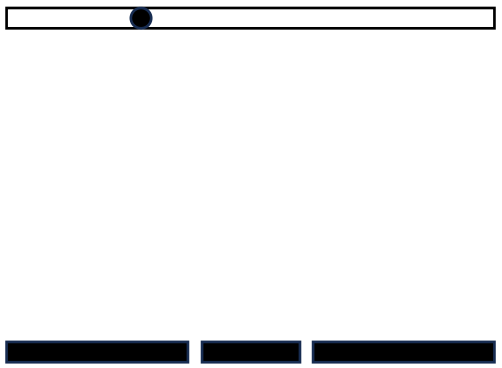
Therefore, light must be particles! ????

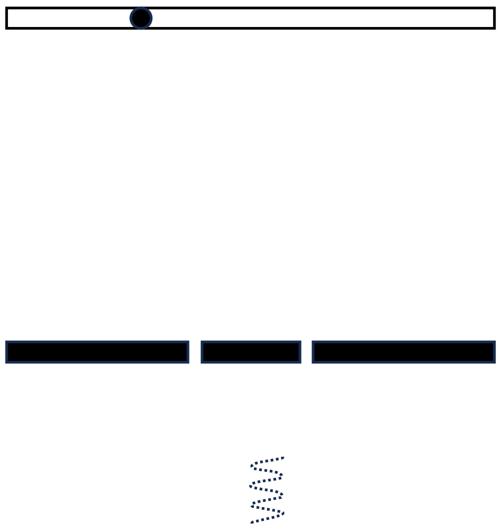
Wave-particle duality

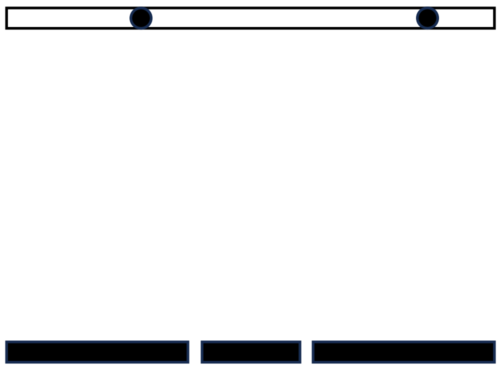
Light (as well as all matter) behave
as both waves and particles

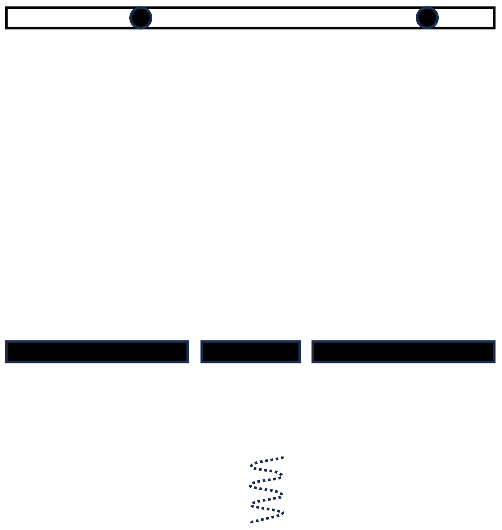
What about Young’s double slit experiment?

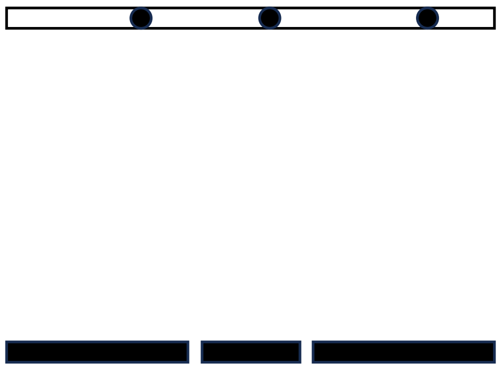
One photon at a time



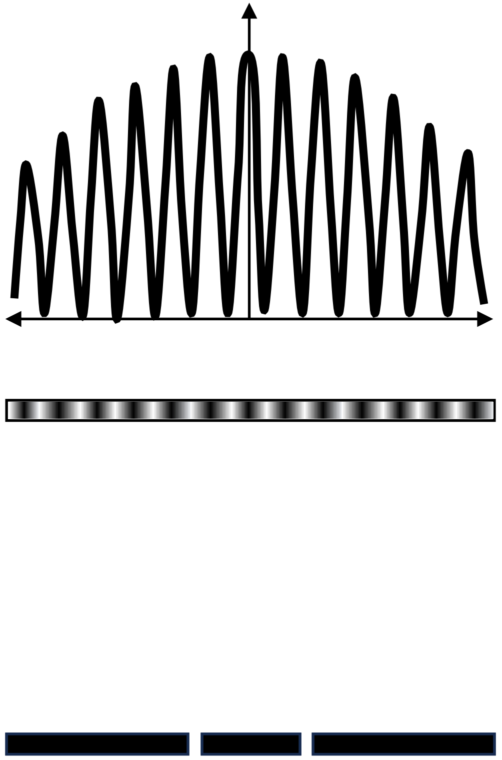








Eventually



Only conclusion is that each photon goes through *both* slits an interfering with *itself*

An abstract framework for quantum mechanics

First, complex numbers

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

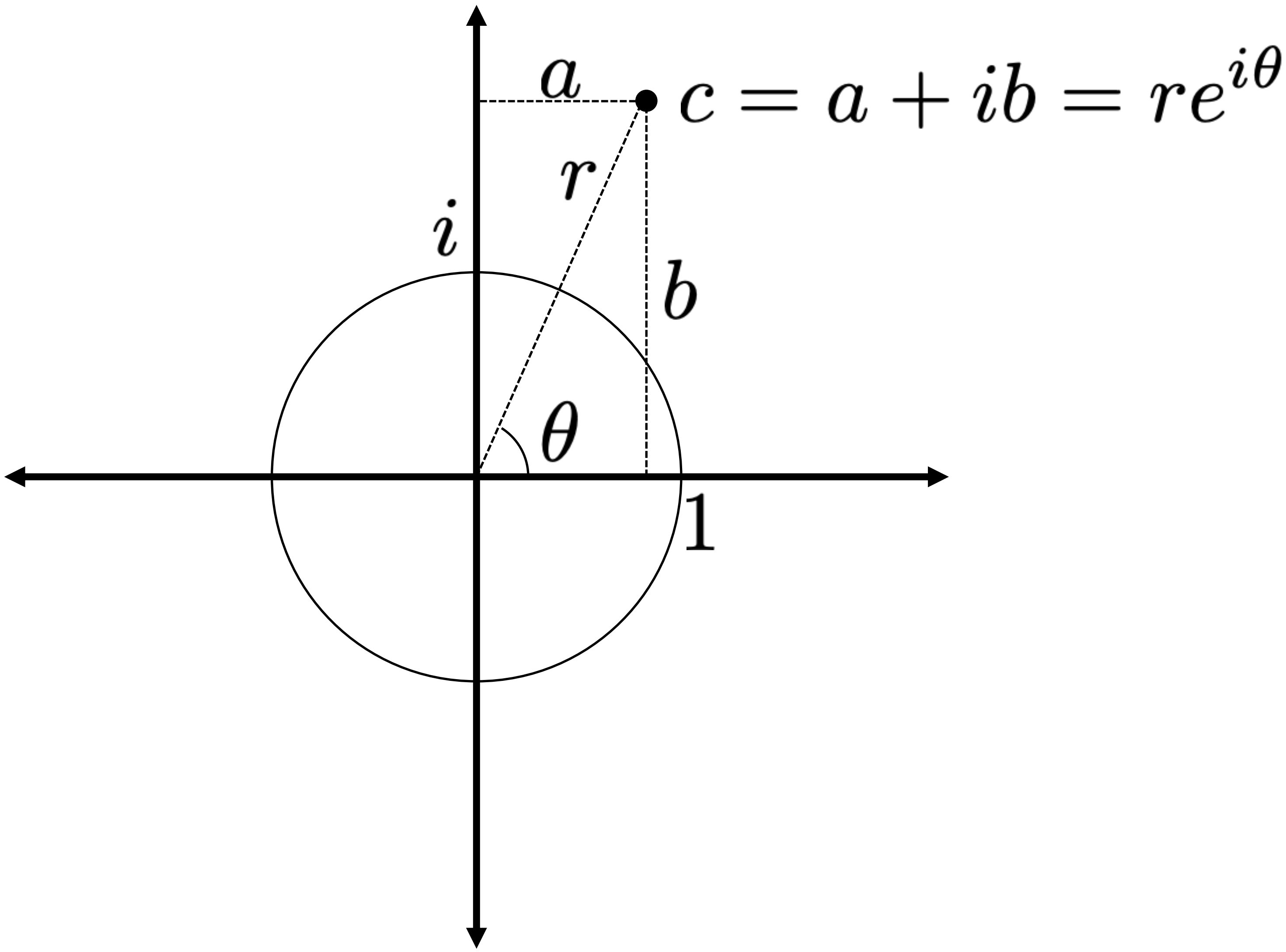
Complex number: $c = a + ib \qquad a, b \in \mathbb{R}$

Conjugate: $c^* = a + i(-b) = a - ib$

Norm: $|c| = \sqrt{a^2 + b^2} = \sqrt{cc^*}$

Euler Identity: $e^{i\theta} = \cos(\theta) + i\sin(\theta)$

Polar coordinates $c = re^{i\theta} = (r\cos(\theta)) + i(r\sin(\theta))$



$c = a + ib = re^{i\theta}$
a
r
i
b
θ
1

Complex Matrices

$$A = \begin{pmatrix} A_{1,1} & A_{1,2} & \cdots \\ A_{2,1} & A_{2,2} & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

Transpose

$$A^T = \begin{pmatrix} A_{1,1} & A_{2,1} & \cdots \\ A_{1,2} & A_{2,2} & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

Conjugate

$$A^* = \begin{pmatrix} A^*_{1,1} & A^*_{1,2} & \cdots \\ A^*_{2,1} & A^*_{2,2} & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

Conjugate Transpose

$$A^\dagger = (A^*)^T = \begin{pmatrix} A^*_{1,1} & A^*_{2,1} & \cdots \\ A^*_{1,2} & A^*_{2,2} & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

Complex Vectors

Column vector

$$v = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \end{pmatrix}$$

Row vector

$$w = \begin{pmatrix} w_1 & w_2 & \cdots \end{pmatrix}$$

Inner products:

$$\langle v, w \rangle = v^\dagger \cdot w$$

$$|v| = \sqrt{\langle v, v \rangle} = \sqrt{v^\dagger \cdot v}$$

Bra-Ket Notation

Column vector

$$|\psi\rangle = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \end{pmatrix}$$

Row vector

$$\langle\psi| = (|\psi\rangle)^\dagger$$

Inner products:

$$\langle\psi|\phi\rangle = \langle\psi| \cdot |\phi\rangle$$

$$|\ |\psi\rangle\ | = \sqrt{\langle\psi|\psi\rangle}$$

Bra-Ket Notation

Standard (computational) basis vectors

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \end{pmatrix} \quad |2\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ \vdots \end{pmatrix} \quad \cdots$$

General vector: $|\psi\rangle = \sum_i \alpha_i |i\rangle$

The State of a Quantum System

Travel through left slit = $|0\rangle$ $|1\rangle$ = Travel through left slit

Photon of “intensity” = 1

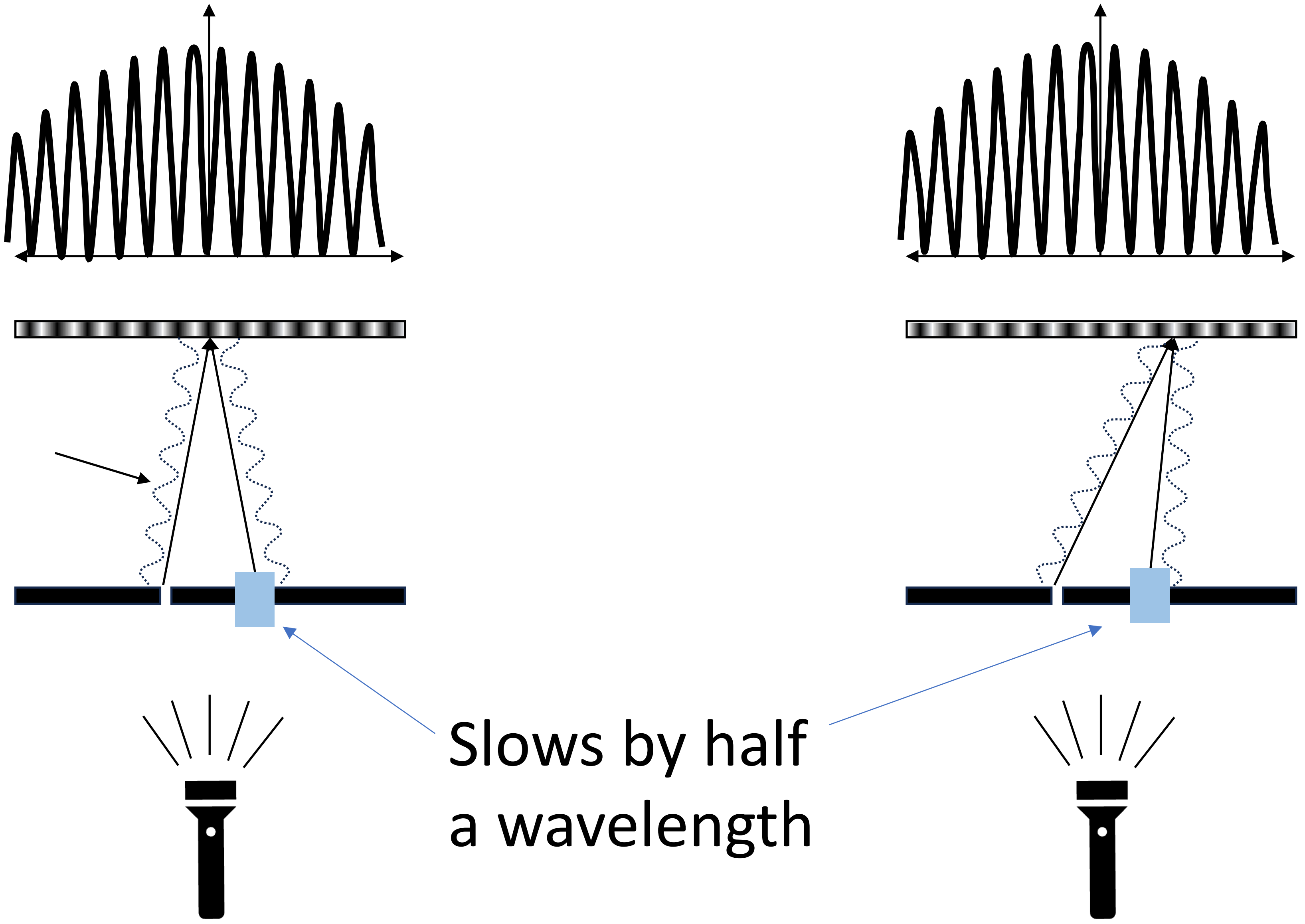
General state of photon: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

α, β represent underlying wave amplitude at each slit

Intensity = |Wave|^2: $|\ |\psi\rangle\ |^2 = \langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2 = 1$

In double slit experiment, $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

Why complex amplitudes?



Why complex amplitudes?

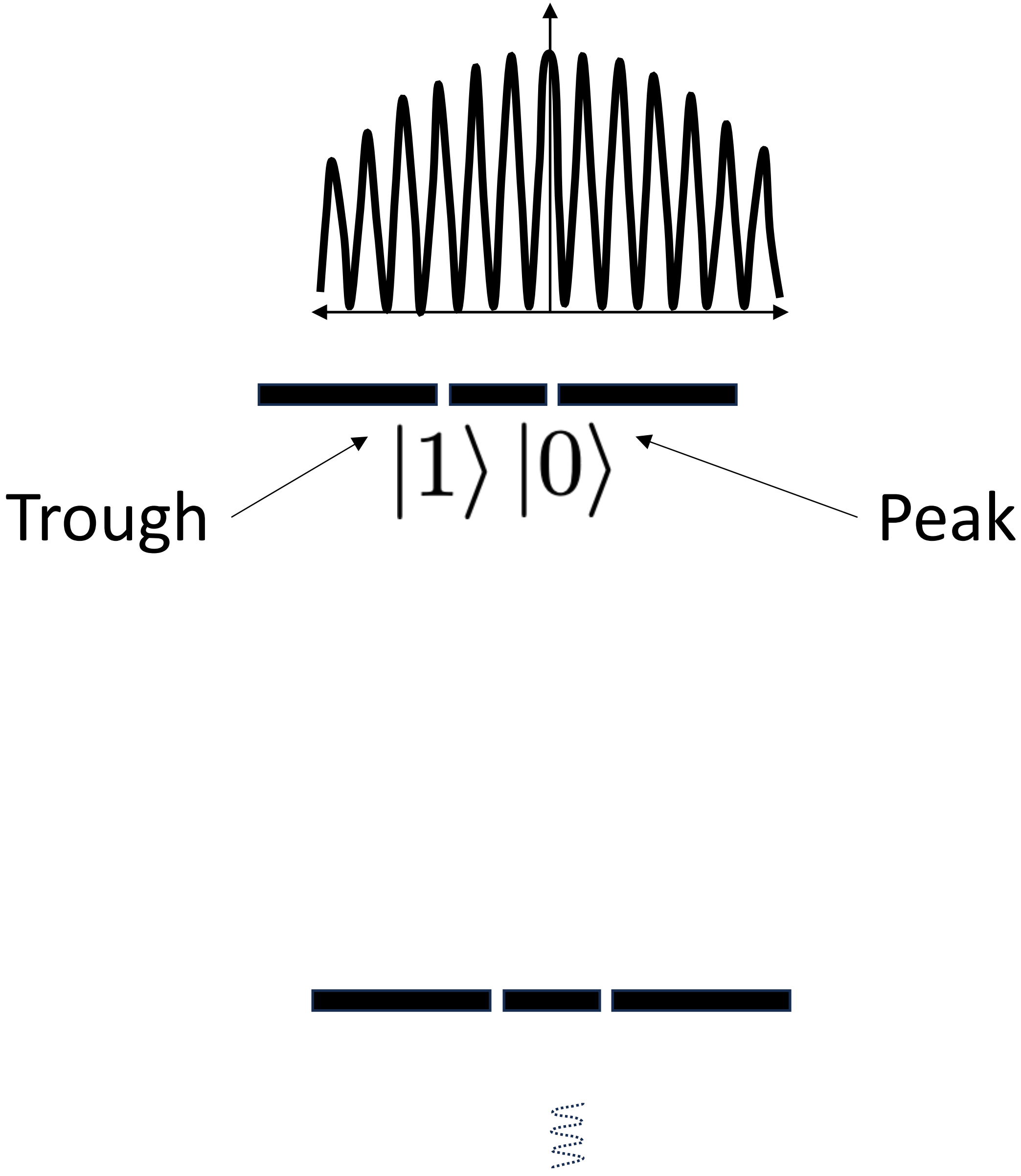
$$\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

In general, delay by fraction of wavelength incurs a complex phase $e^{i\theta}$

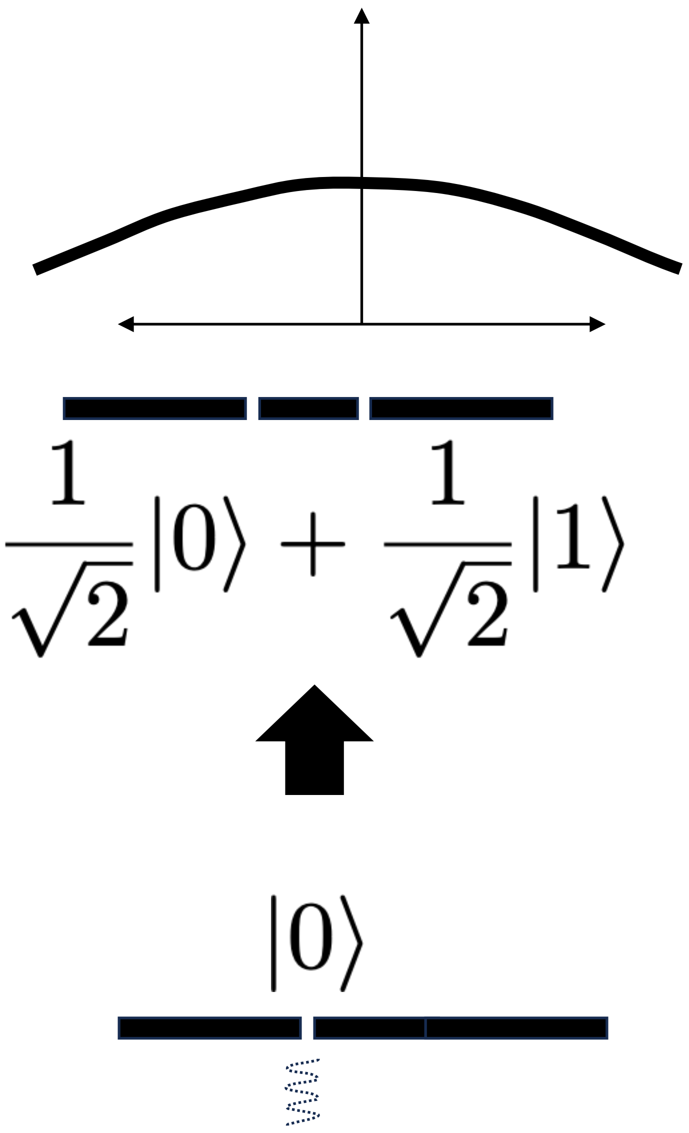
In a general system, quantum state
is an arbitrary vector of unit norm

Operations on quantum states

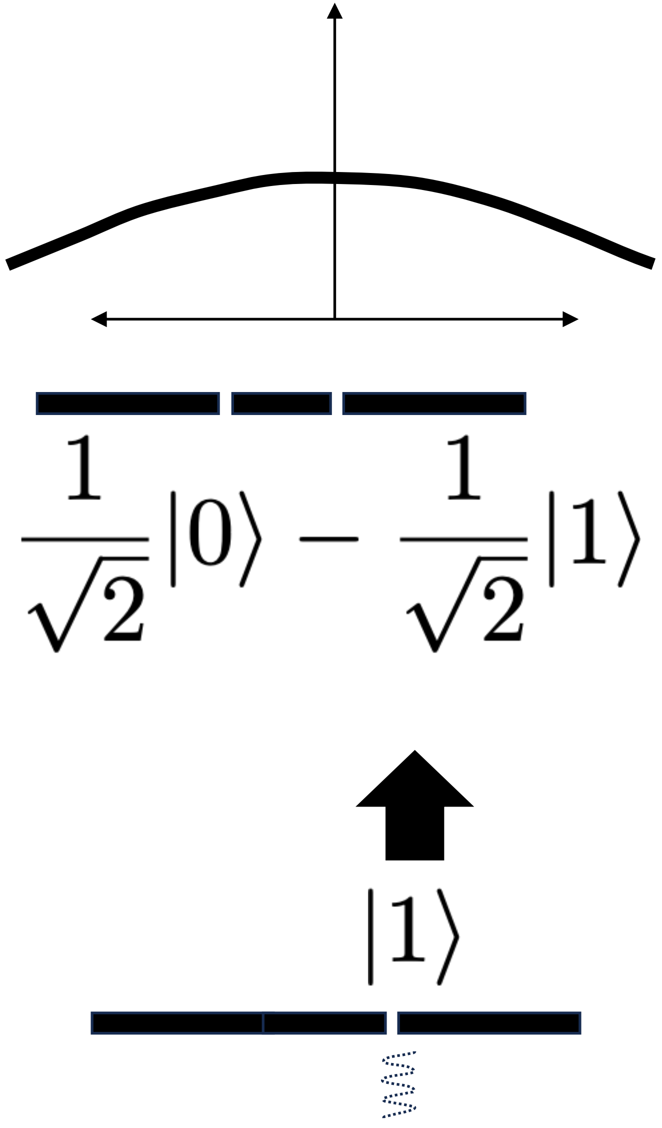
Assume that we normalize state at second wall



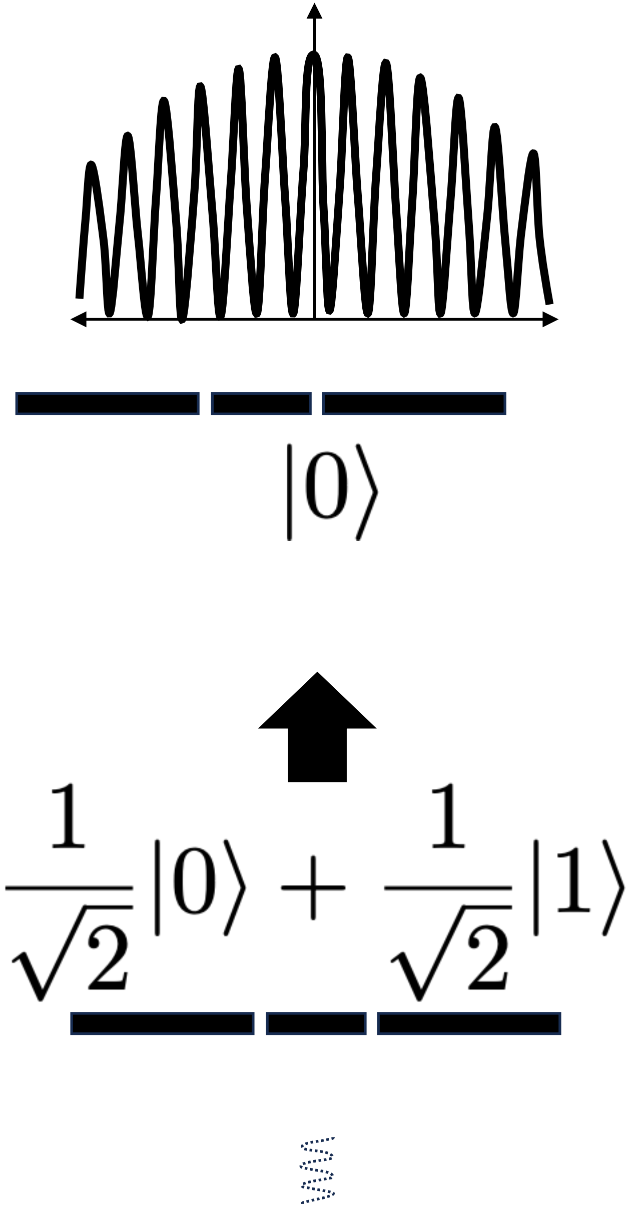
First slit of first wall gives equal contributions to both slits at second wall



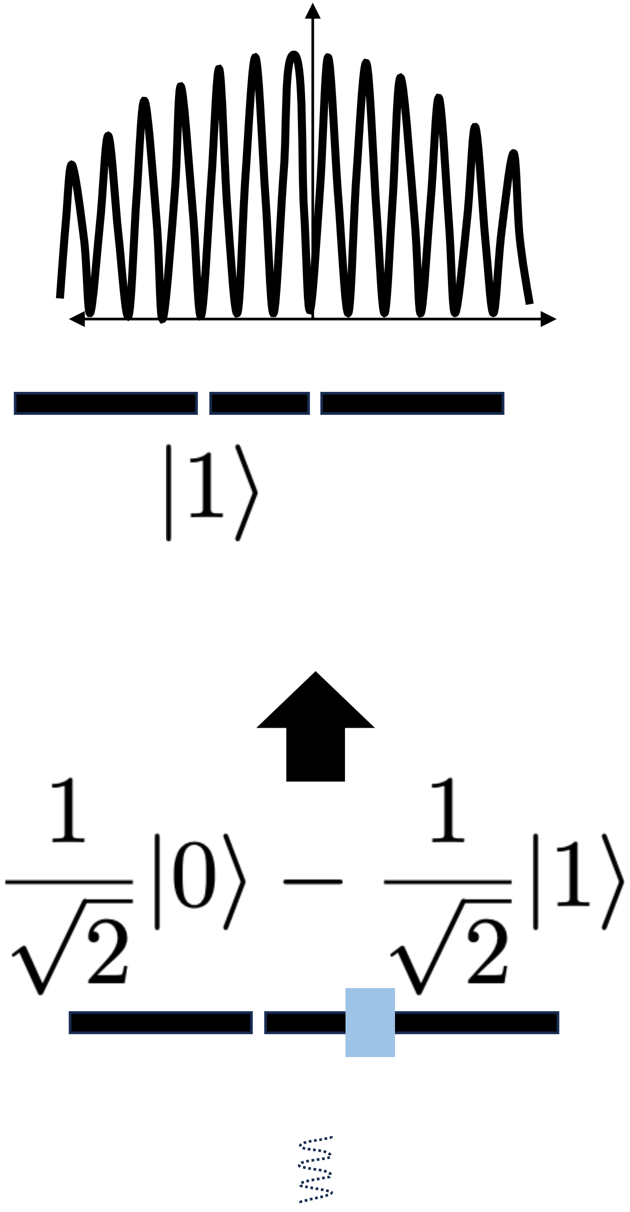
First slit of first wall gives equal contributions to both slits at second wall, but “out of phase” due to different path lengths



Interference puts entire field at one slit



Putting the two slits out of phase shifts the interference pattern



In general, waves add linearly, so we can work out the transformation for any state

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \Rightarrow \left(\frac{\alpha+\beta}{\sqrt{2}}\right)|0\rangle + \left(\frac{\alpha-\beta}{\sqrt{2}}\right)|1\rangle$$

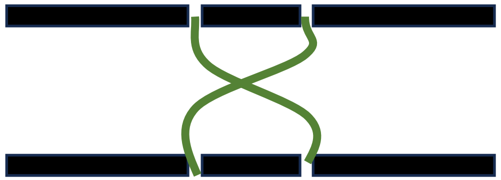
$$= \mathbf{H}|\psi\rangle$$

$$\mathbf{H} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

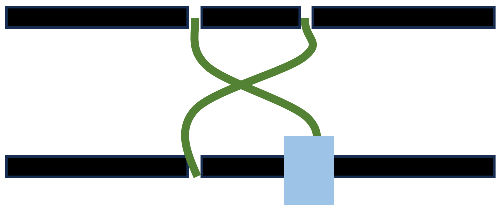
Called "Hadamard Transform"

Other transforms possible as well:

$$\mathbf{P}(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$



$$\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$



$$\mathbf{XP}(\theta) = \begin{pmatrix} 0 & e^{i\theta} \\ 1 & 0 \end{pmatrix}$$

A quantum transformation is a linear transformation:

$$|\psi\rangle \longrightarrow U|\psi\rangle$$

The only restriction is that the norm of any input state must be preserved

$$\langle\psi|\psi\rangle = (U|\psi\rangle)^\dagger(U|\psi\rangle) = \langle\psi|U^\dagger U|\psi\rangle$$

$$\Longrightarrow U^\dagger U = \mathbf{I}$$

A quantum transformation is a ~~linear~~ transformation:
unitary*

$$|\psi\rangle \Longrightarrow U|\psi\rangle$$

A unitary matrix U is square and satisfies $U^\dagger U = \mathbf{I}$

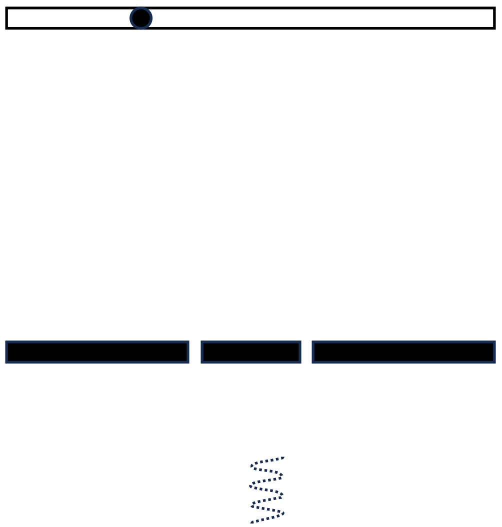
Or equivalently $U^{-1} = U^\dagger$

In particular, the inverse always exists

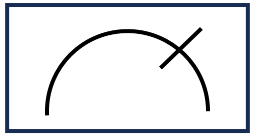
* ok, technically the transformation doesn't need to be square, in which case its called an "isometry".
But any isometry can be "filled out" into a unitary. So for this course, we will focus on unitaries

Measuring a Quantum System

Recall:



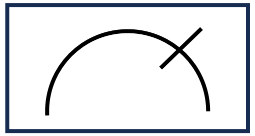
The photon being detected is a *measurement* that “collapses” the photon so that it is at a single location

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow$$  $$\rightarrow$$

0 w/ probability $|\alpha|^2$

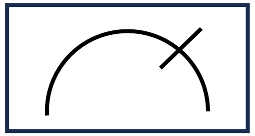
1 w/ probability $|\beta|^2$

Normalization ensures valid probability distribution, and squaring matches the relationship between underlying wave and observed intensity/probability

In general: $|\psi\rangle \rightarrow$  $\rightarrow$ i w/ probability $|\langle i|\psi\rangle|^2$

Post-measurement state of system

Rather than a measurement destroying the state, we will usually think of it as simply "collapsing" the state to be at a given location; the state can then be further acted on

$|\psi\rangle$ $\Rightarrow$  $\Rightarrow$ i w/ probability $|\langle i|\psi\rangle|^2$

Then state collapses to $|i\rangle$

Up Next: Quantum key distribution (Quantum meets cryptography)