UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

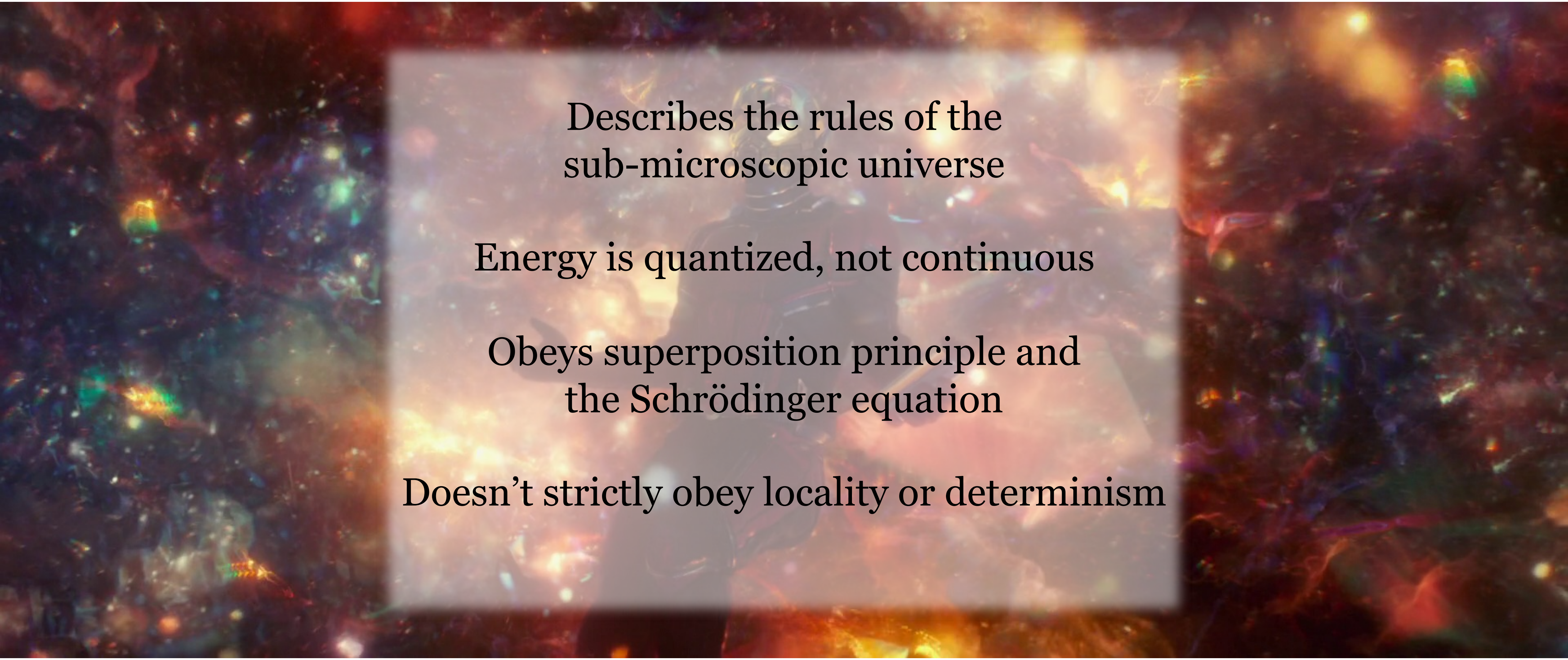
Math Circles 2023

Grover's Algorithm I

John Donohue & Sarah Meng Li

Acknowledgement: We are very grateful to Dr. John Donohue for sharing the slides with us. This was created for Quantum School for Young Students (QSYS) 2022.

The Quantum Realm



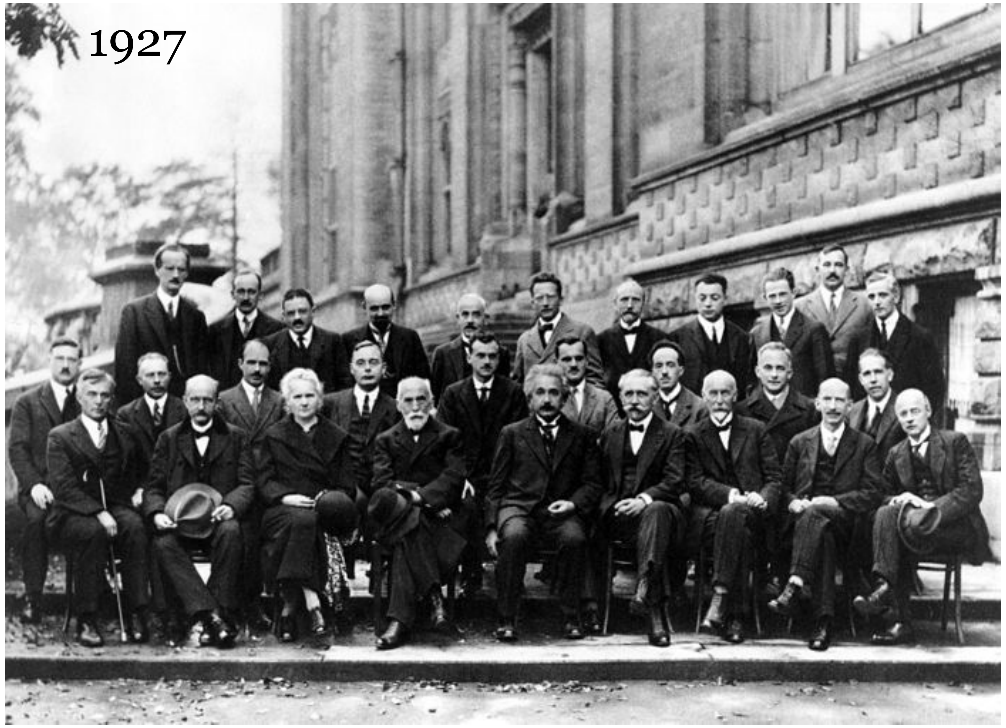
Describes the rules of the sub-microscopic universe

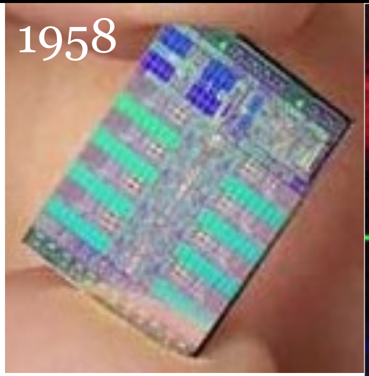
Energy is quantized, not continuous

Obeys superposition principle and the Schrödinger equation

Doesn’t strictly obey locality or determinism

Old-Hat Quantum





Quantum science has been around a long time,
and has already produced many key technologies.

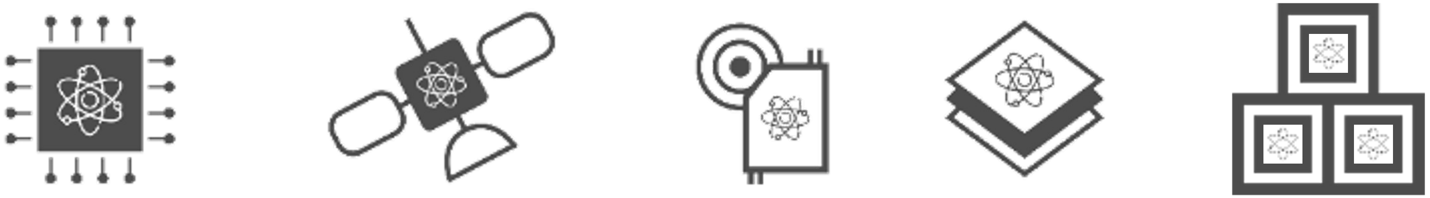
QUANTUM INFORMATION SCIENCE

A field that uses principles like superposition to transform information in new ways, with elements of:

- Computer Science
- Mathematics
- Cryptography
- Chemistry
- Physics
- Engineering

and more!

Applications include…



Computing | Communication | Sensors | Materials | Foundations

The Institute for Quantum Computing at the University of Waterloo

32 independent research groups
Over 150 graduate students

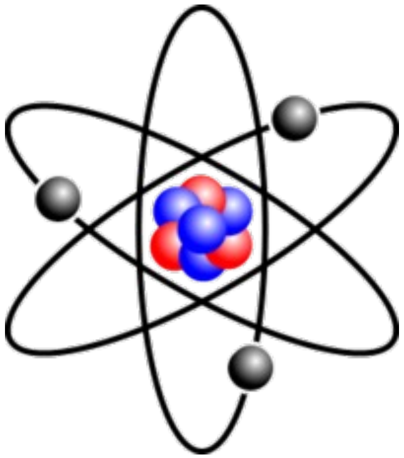
Representation from:
Physics / Chemistry / Electric Engineering / Computer Science
Pure Mathematics / Applied Mathematics / Combinatorics & Optimization

@QUANTUMIQC
www.iqc.ca

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

What makes quantum difficult?

Reason #1:
It's hard to "see"



Reason #2:
It involves math

$$\frac{-\hbar^2}{2m}\nabla^2\psi(\vec{x}) + V(\vec{x})\psi(\vec{x}) = E\,\psi(\vec{x})$$

$$U|\psi\rangle_A \otimes V|\phi\rangle_B$$

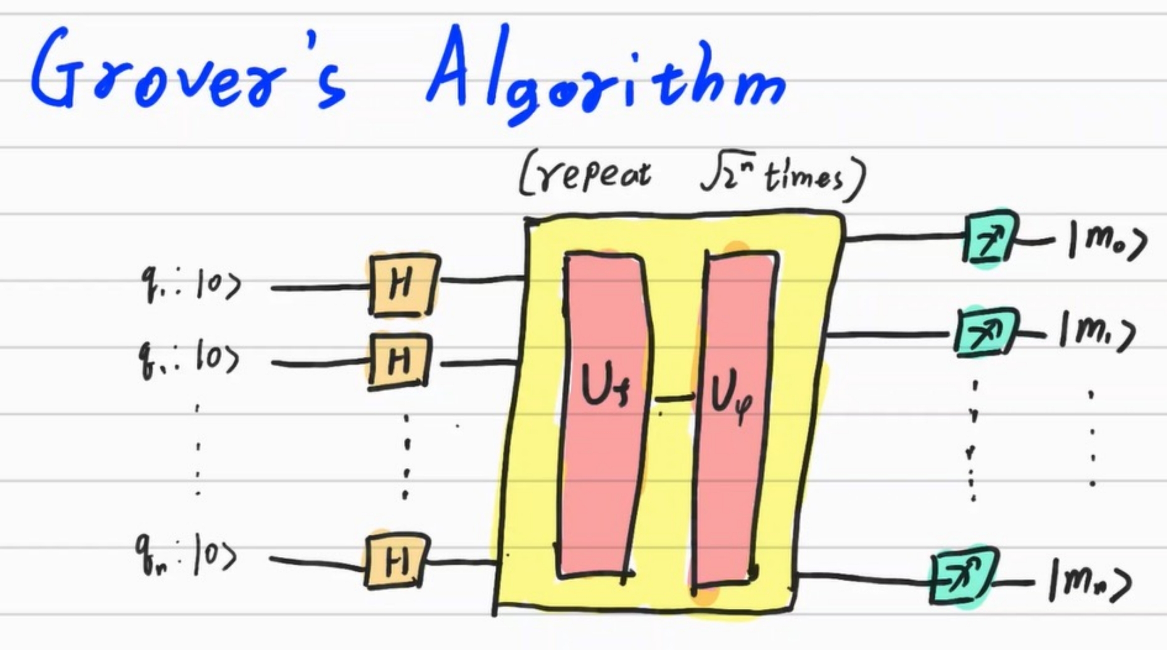
$$U \otimes V = \begin{bmatrix} u_1v_1 & u_1v_2 & u_2v_1 & u_2v_2 \\ u_1v_3 & u_1v_4 & u_2v_3 & u_2v_4 \\ u_3v_1 & u_3v_2 & u_4v_1 & u_4v_2 \\ u_3v_3 & u_3v_4 & u_4v_3 & u_4v_4 \end{bmatrix} = \begin{bmatrix} u_1V & u_2V \\ u_3V & u_4V \end{bmatrix}$$

$$A = (E_g) \times |g\rangle\langle g| + (E_e) \times |e\rangle\langle e|$$

$$P(\phi) = |\langle\phi|\psi\rangle|^2$$

Today's Session

- Review Complex Numbers
- Introduce Vectors
- Motivate the Grover's Algorithm

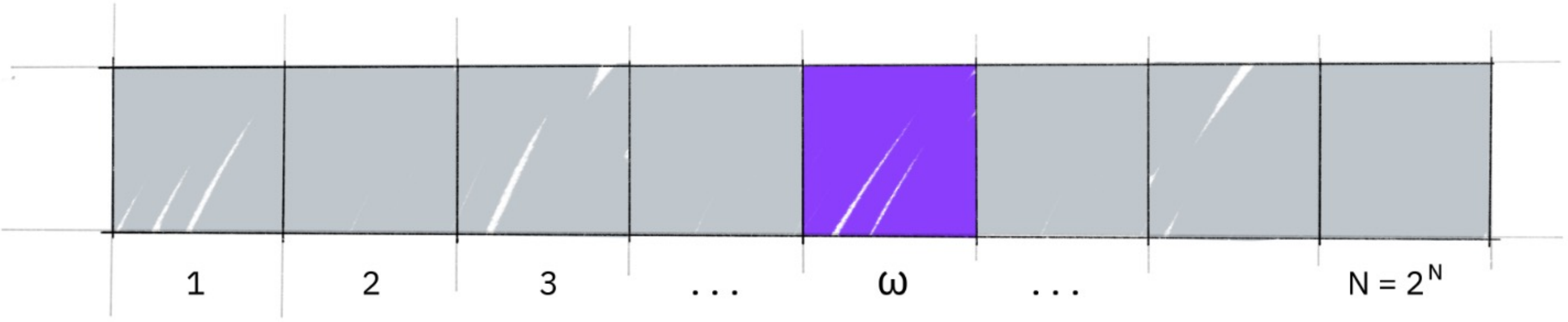


Search in an unstructured database

FROM $O(N)$ TO $O(\sqrt{N})$

Unstructured Search

Suppose you are given a large list of N items. Among these items there is one item with a unique property that we wish to locate; we will call this one the winner w. Think of each item in the list as a box of a particular color. Say all items in the list are gray except the winner w, which is purple.

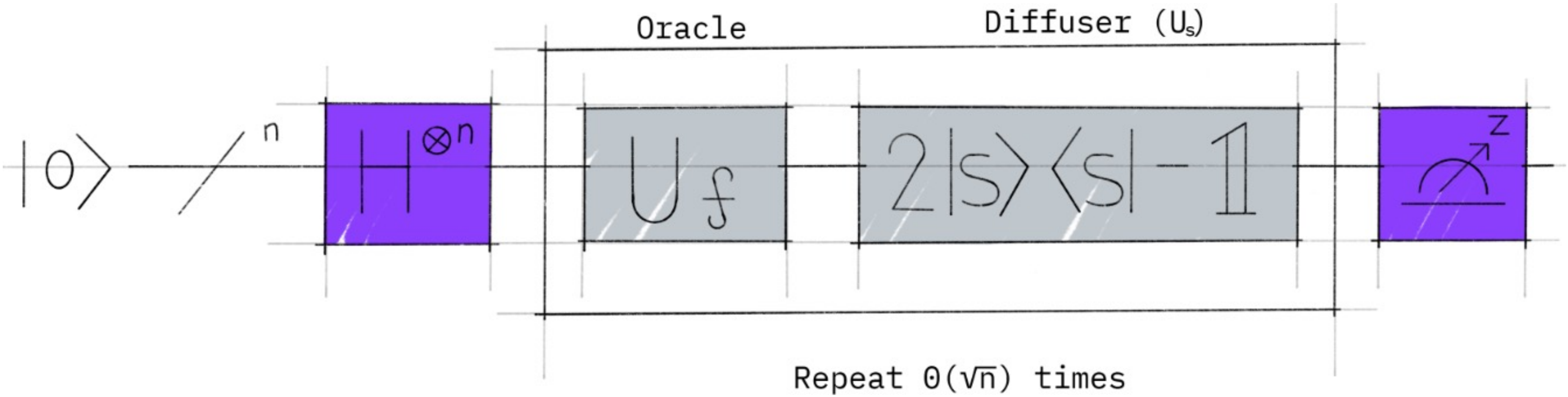


Quantum versus Classical

Quantum search algorithm offers a remarkable advantage of quadratic reduction in query complexity using quantum superposition principle.

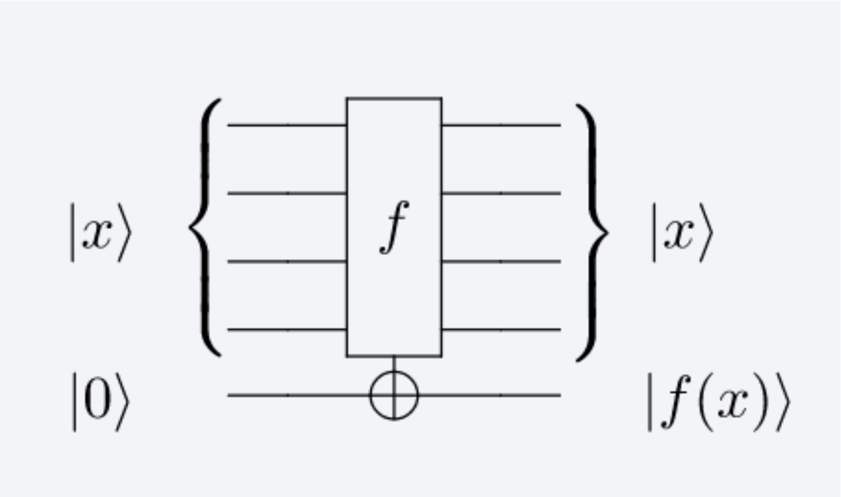
Techniques

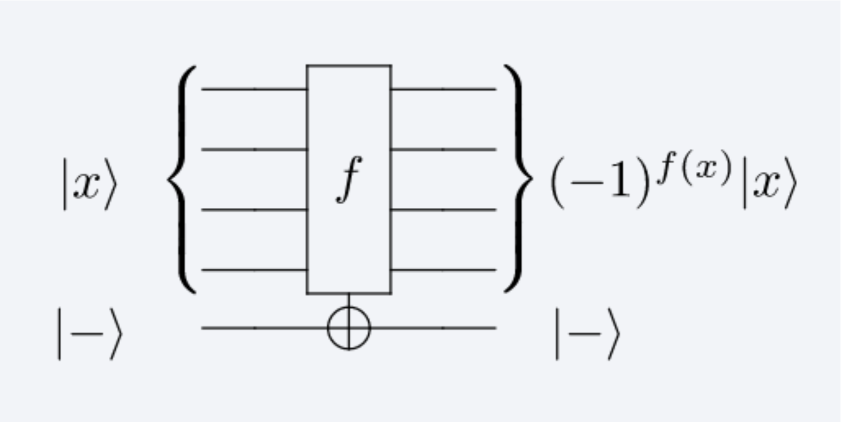
AMPLITUDE AMPLIFICATION & GEOMETRIC INTERPRETATION

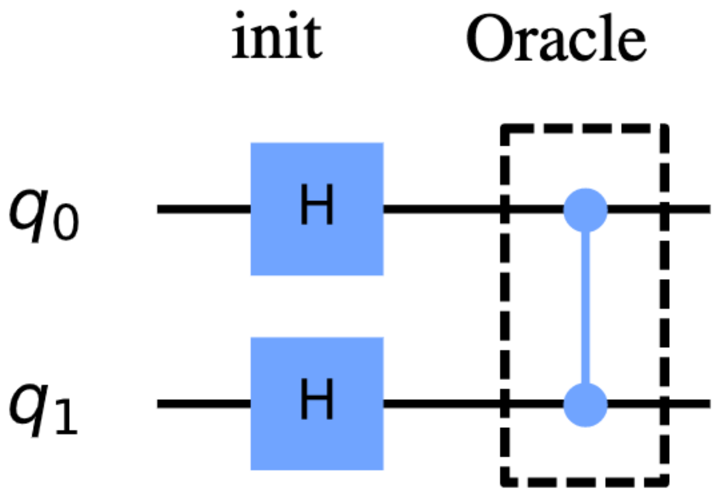

Oracle
Diffuser (U_s)
$|0\rangle$
n
$H^{\otimes n}$
U_f
$2|s\rangle\langle s| - \mathbb{1}$
z
Repeat $O(\sqrt{n})$ times

Big Picture

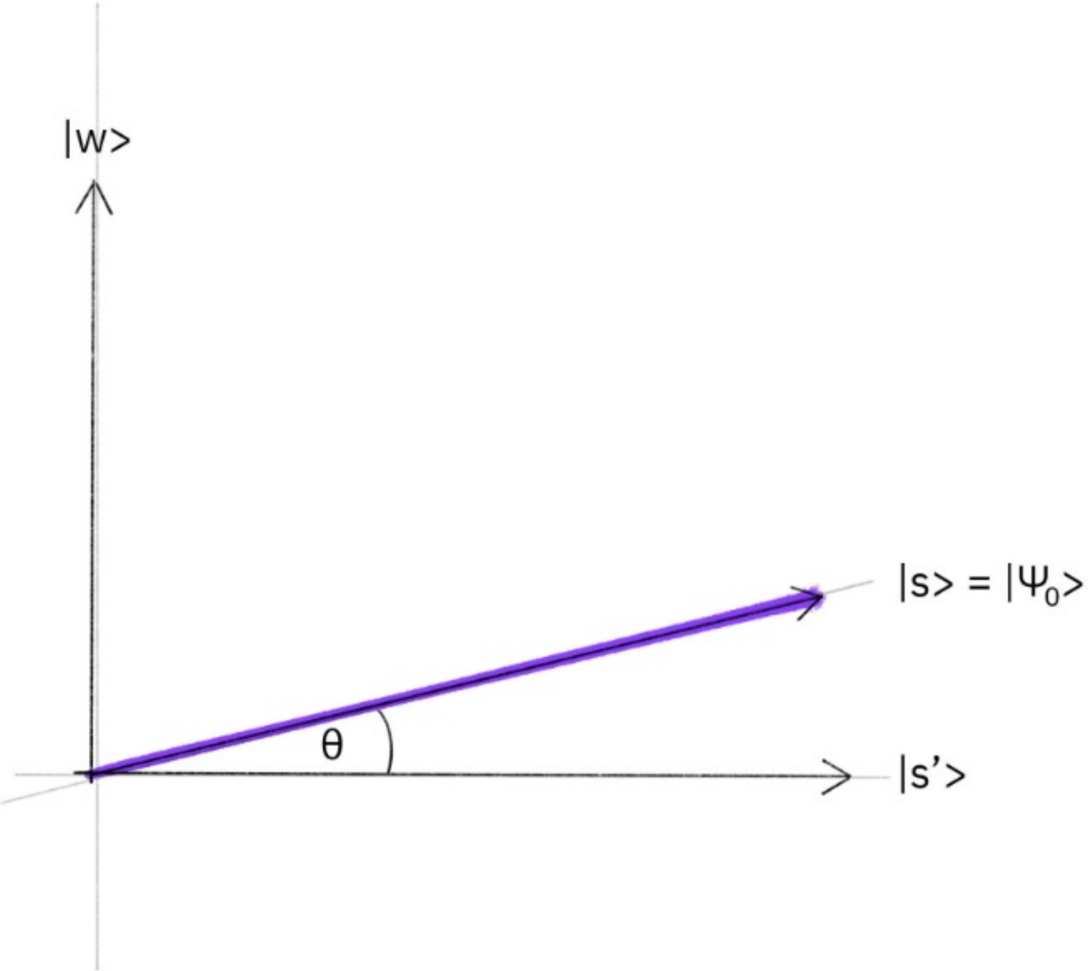
Phase kickback in Grover's oracle

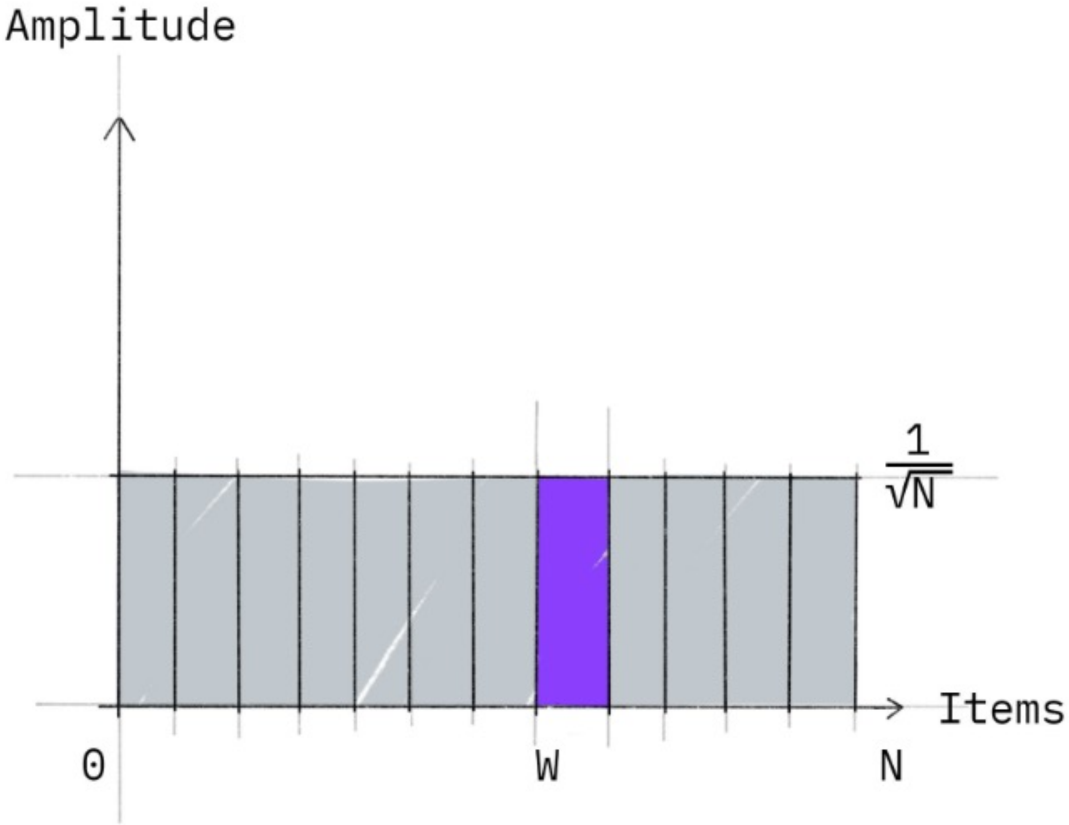




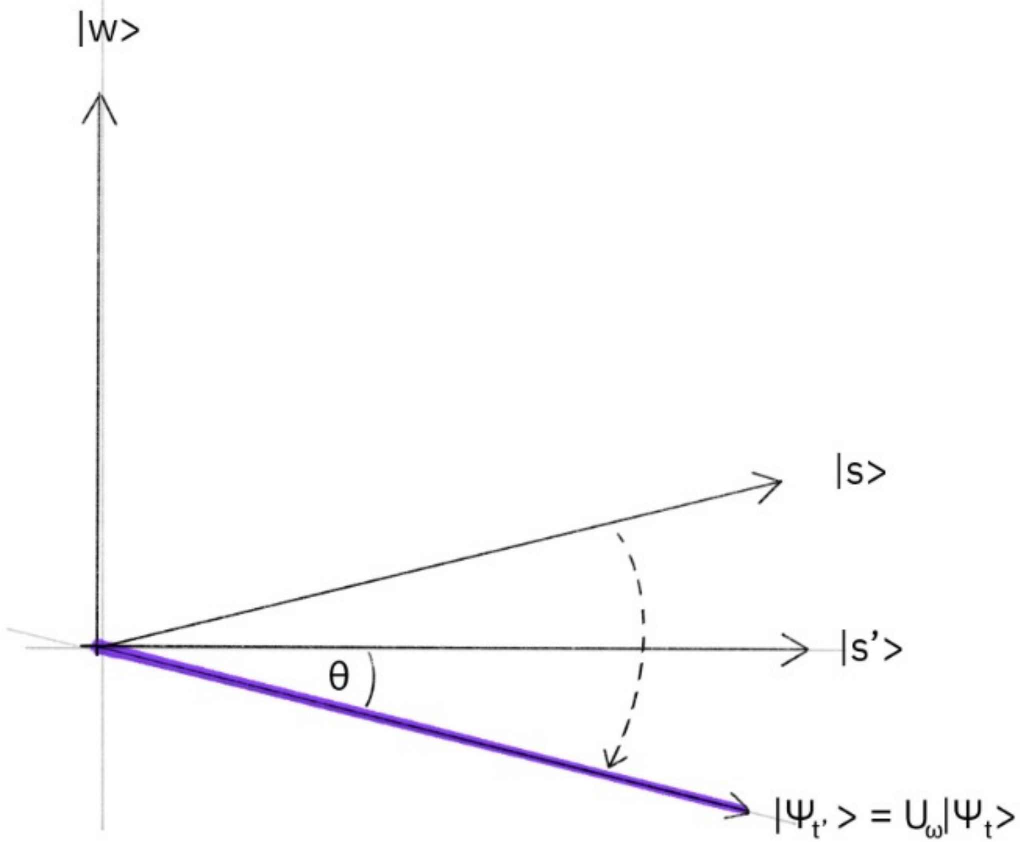


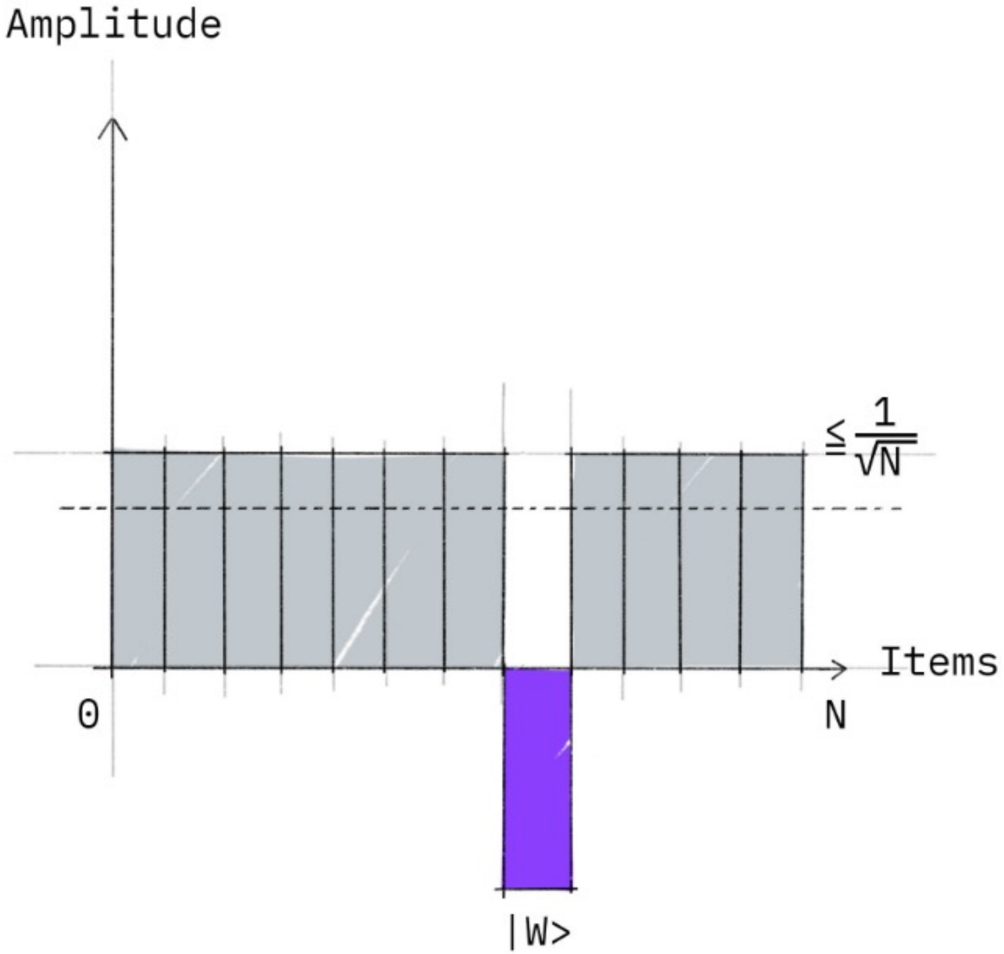
$$U_\omega = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$



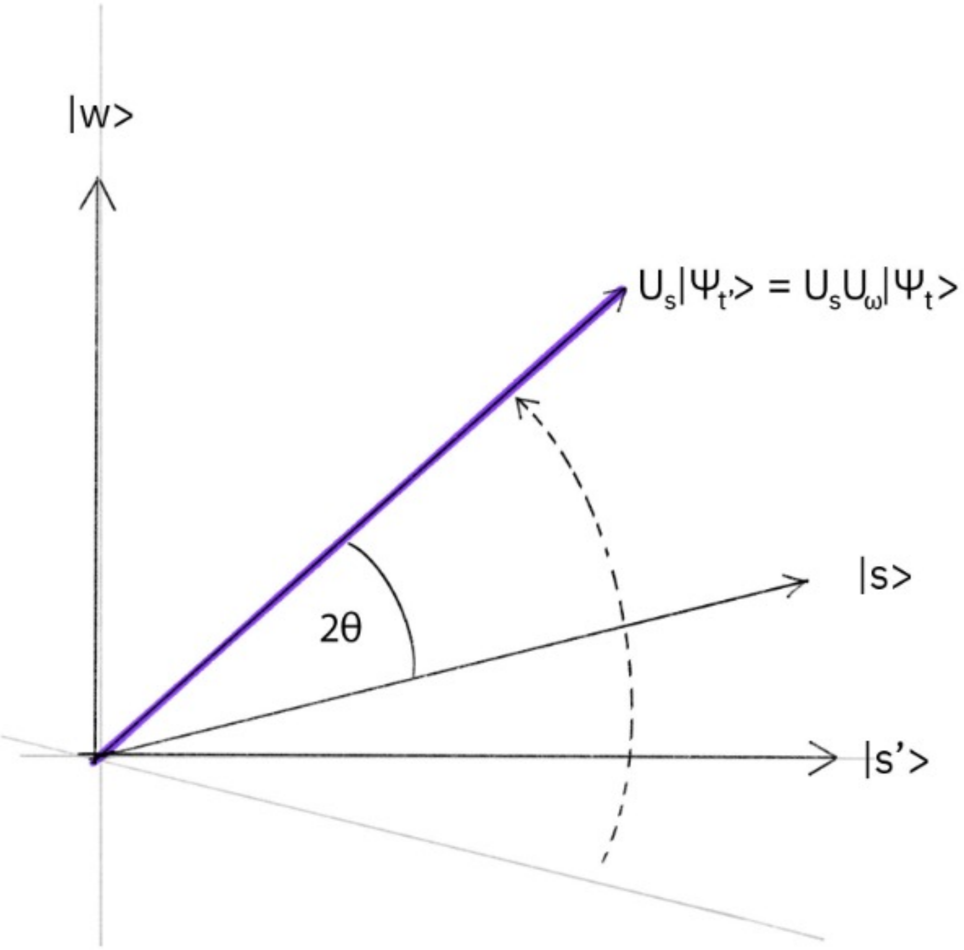


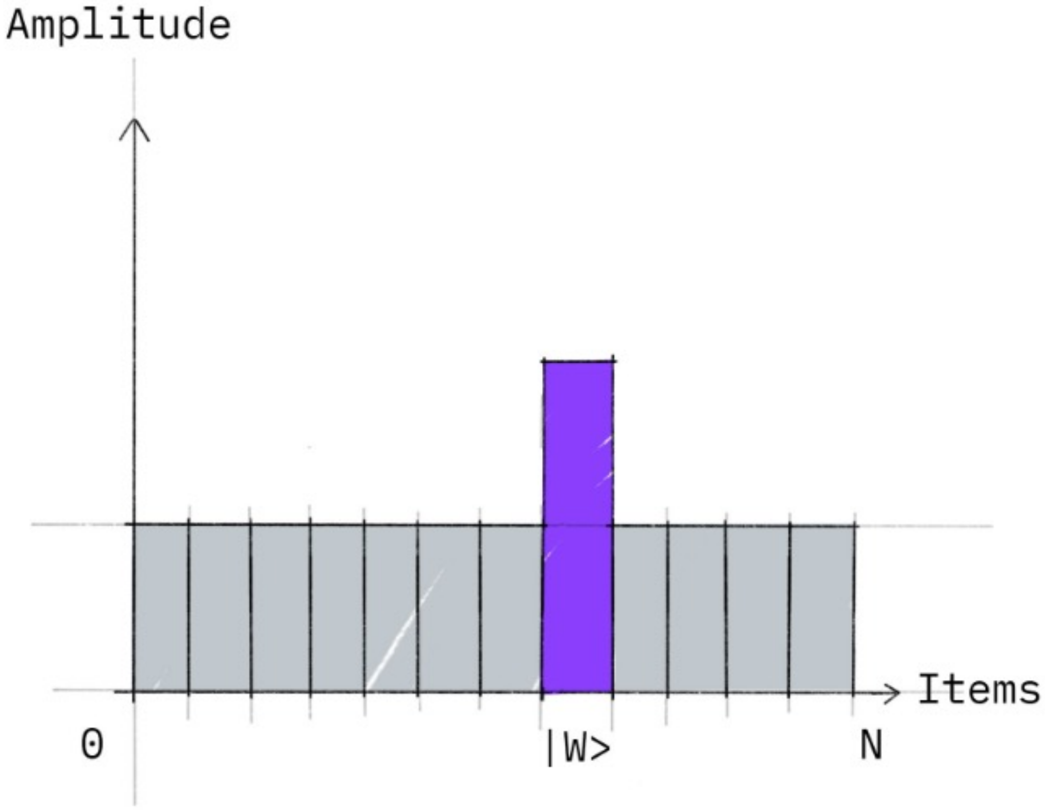
Amplitude amplifications



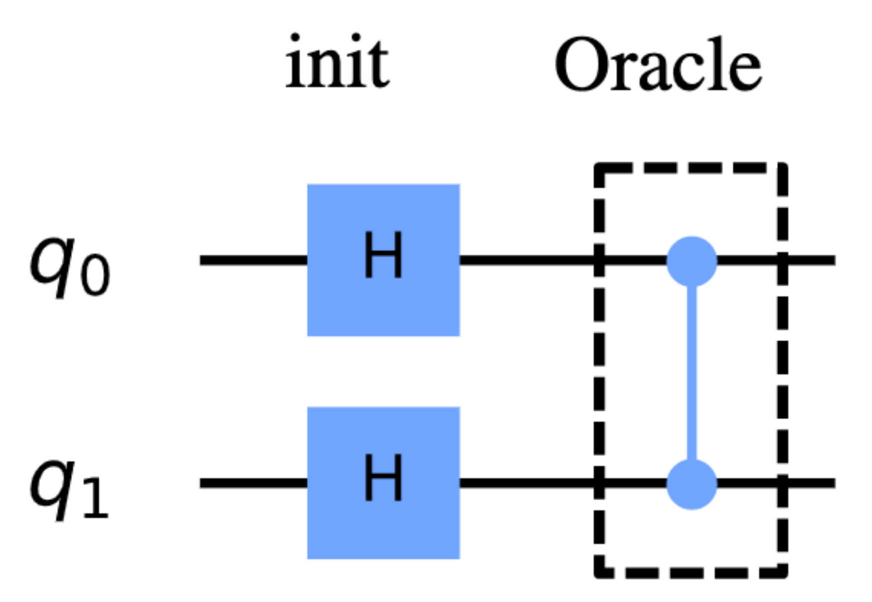


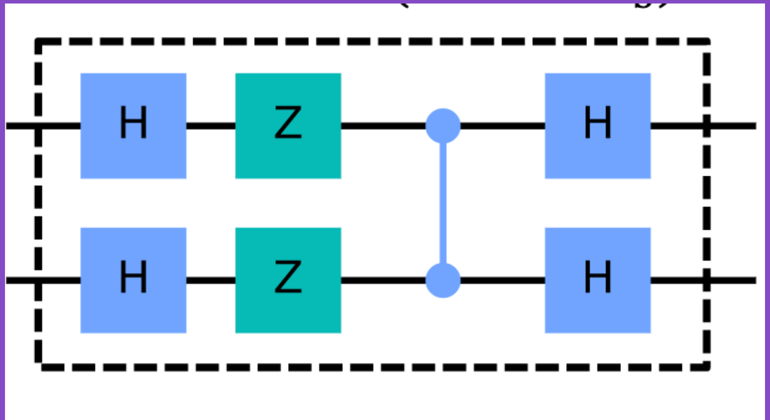
Amplitude amplifications





Amplitude amplifications

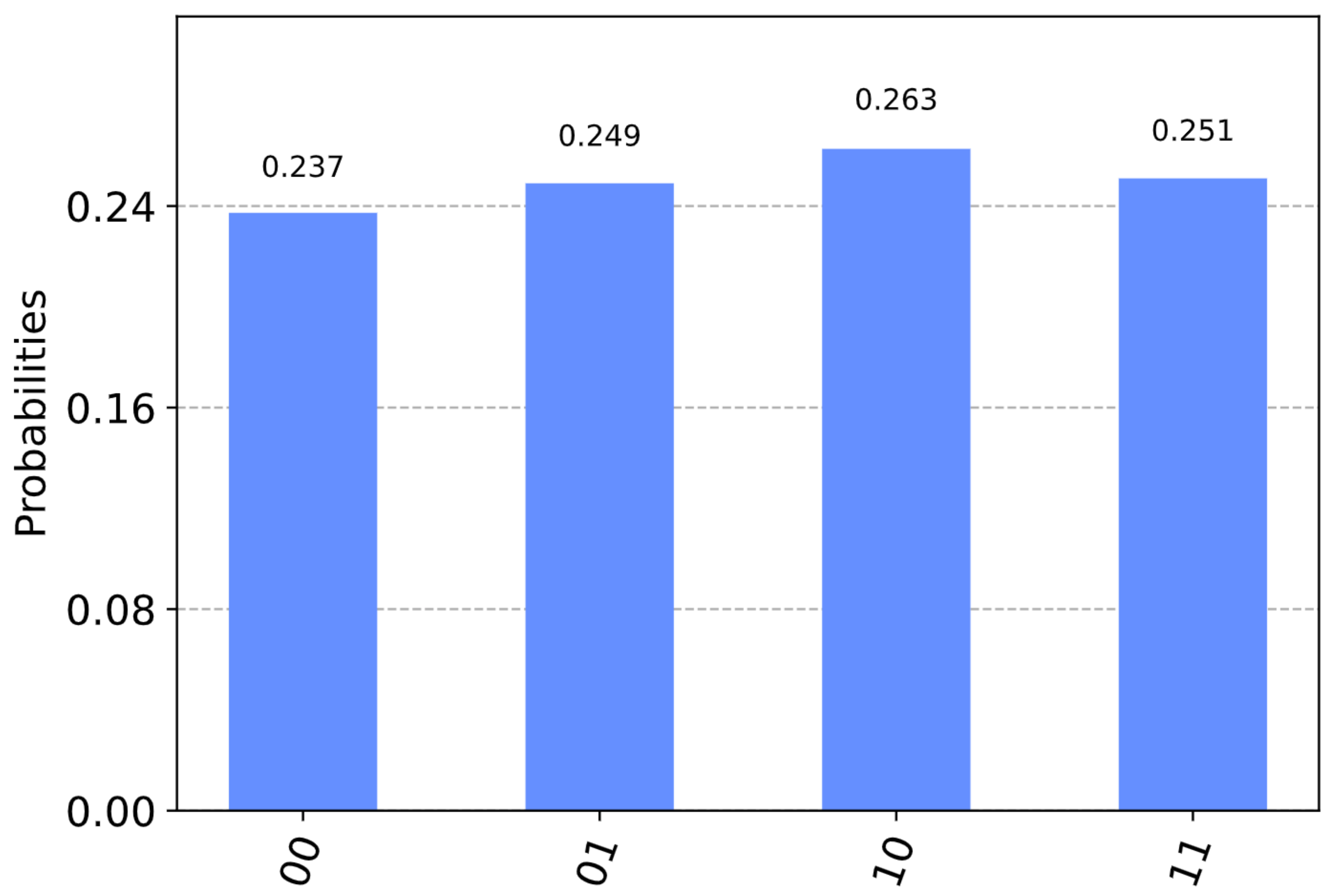


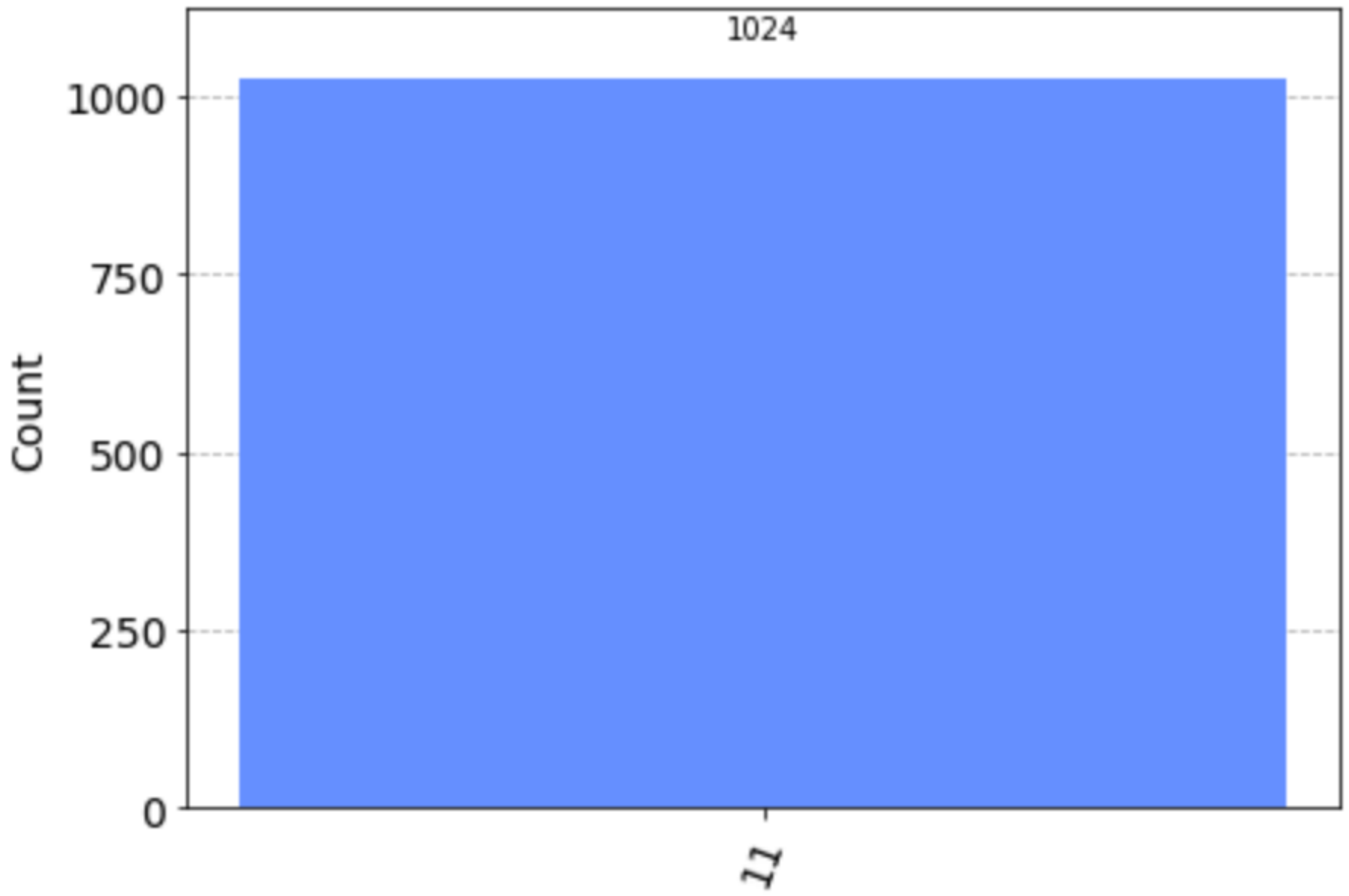


Grover's Oracle + Diffuser

Amplitude amplification stretches out (amplifies) the amplitudes of the marked items.

It shrinks other elements' amplitude.

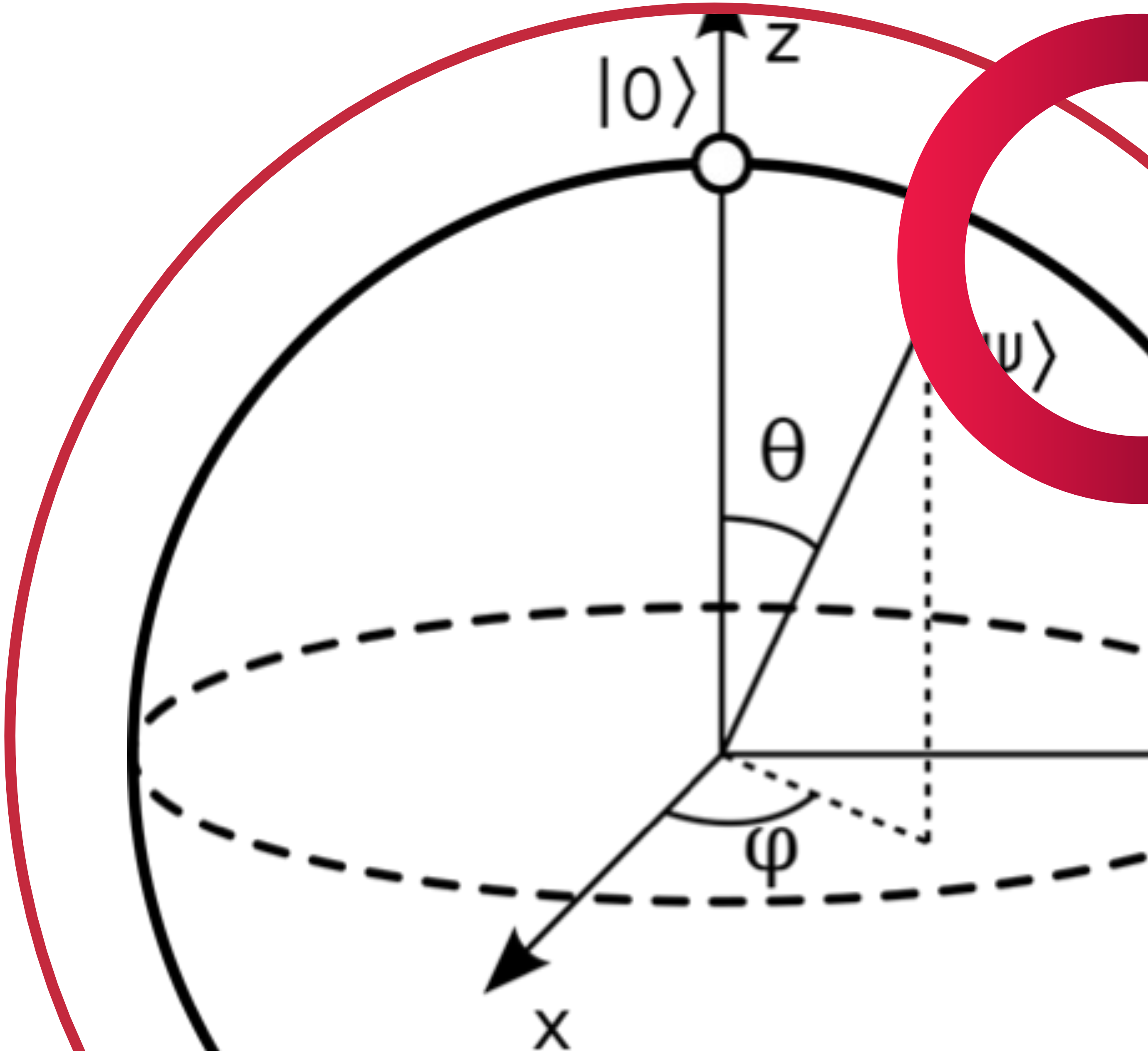

0.237
0.249
0.263
0.251
0.24
0.16
0.08
0.00
Probabilities
00
01
10
11


1024
1000
750
500
250
0
Count
11

THE POSTULATES OF QUANTUM MECHANICS

John Donohue

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing



The terms “real” and “imaginary” [numbers] are relics from the days when these concepts had not been formalized, were imperfectly understood, and were generally rather mysterious.

They have quietly been de-mythologized over the years, [and] no scintilla of their common parlance still attaches to them.

Robert B. Burckel

All numbers are imaginary. Even “zero” was contentious once.

The hottest contenders for numbers without purpose are probably the p-adic numbers (an extension of the rationals), and perhaps the expiry dates on army ration packs.

Michael Hall

COMPLEX NUMBERS

How confident do you feel working with **imaginary and complex numbers?**

A. Complex numbers are easy!

B. I'm pretty confident

C. I'm starting to get used to it

D. Complex numbers are difficult

E. I'm completely lost

What are the solutions to $(x^2 - 1) = -10$?

A. $x = 3i$

B. $x = -3$

C. $x = -3i$

D. None of the above

E. Both A & C

What is a solution to $(x-3)^2 = -4$?

A. $x = 2i$

B. $x = 3$

C. $x = 5i$

D. $x = 3 - 2i$

E. $x = 2 + 3i$

Complex Numbers

Complex numbers are a natural extension of the real numbers, able to handle a wide variety of problems in physics and engineering.

Real unit:	1
Imaginary unit:	$i = \sqrt{-1}$

A **complex number** has both real and imaginary parts, where a and b are real numbers.

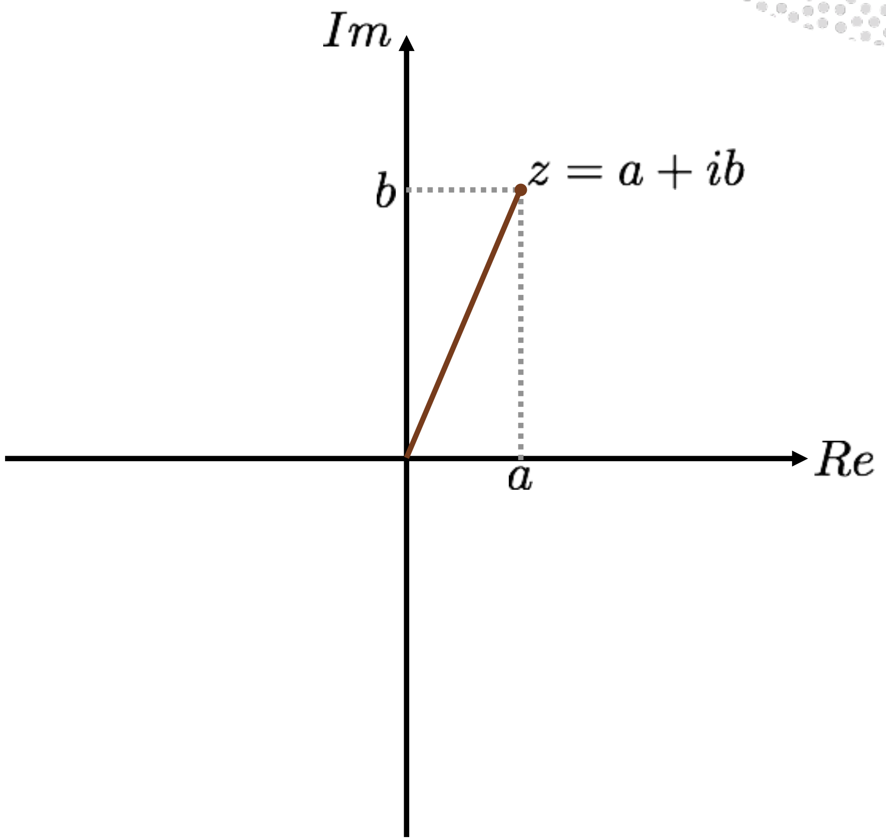
$$z = a + ib$$

A complex number z can be broken into real and imaginary parts, a and ib

An imaginary number has no real part

A real number has no imaginary part

The Complex Plane
A 2D extension of the number line



What is $(2 + 2i) - (5 - 3i)$?

A. $7 + 5i$

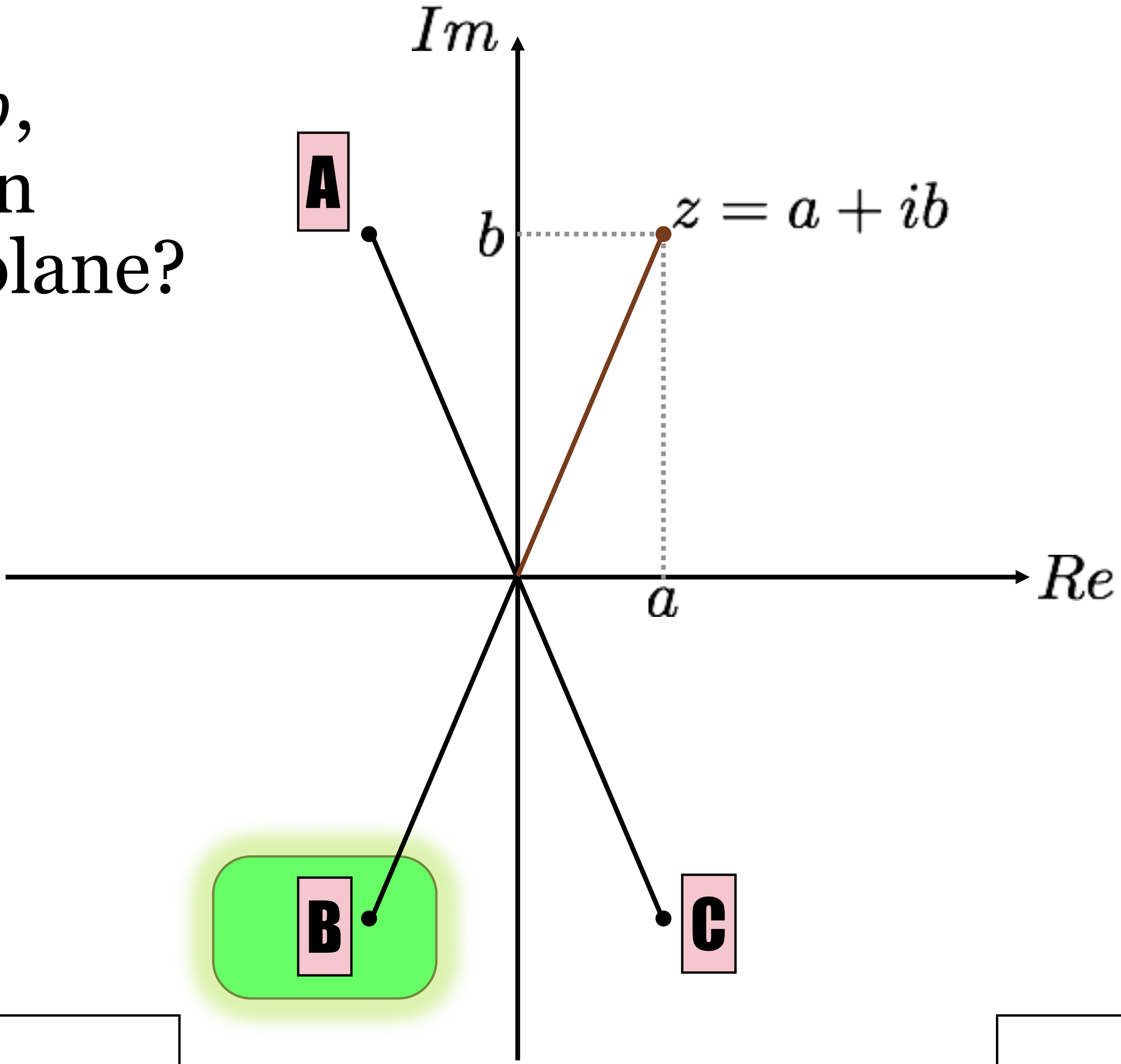
B. $7 - i$

C. $-3 + 5i$

D. $3 - 5i$

E. None of the above

For $z = a + ib$, where is $-z$ on the complex plane?



D.
Not enough information

E.
None of the above

The Complex Conjugate

The complex conjugate is the complex number with the imaginary part negated,

If z $= a + ib$, then $\bar{z} = a - ib$

We can use this to find various properties of the complex number:

$$Re(z) = \frac{z + \bar{z}}{2} = a$$

$$Im(z) = -i \times \frac{(z - \bar{z})}{2} = b$$

$$Abs(z) = \sqrt{z\bar{z}} == \sqrt{a^2 + b^2}$$

What is the complex conjugate of $(3+2i)\times(4-i)$?

A. $14-5i$

B. $14+5i$

$$(3+2i)(4-i) = 12-3i+8i-2i^2$$

$$10-5i = 14+5\mathbf{i}$$

$$\overline{(3+2i)(4-i)} = 14-5\mathbf{i}$$

OR

$$\overline{(3+2i)(4-i)} = (3-2i)(4+i)$$

$$10+5i$$

$$= 12-3i+8i-2i^2$$

$$= 14+5\mathbf{i}$$

E. None of the above

What is
$2 \div (1 + 3i)$?

A. $3 + i$

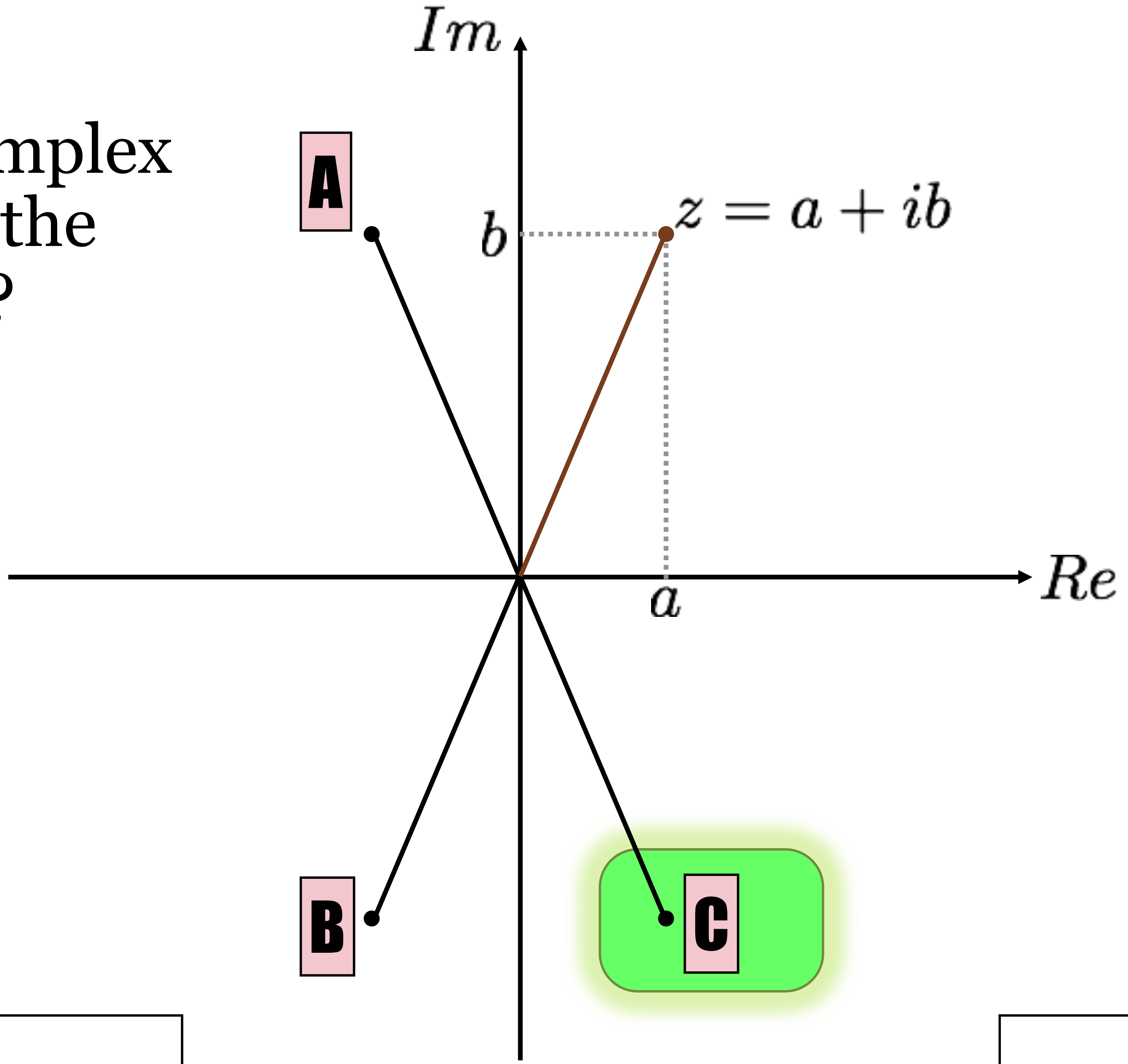
B. $\frac{3 + i}{5}$

C. $\frac{1 + 3i}{5}$

D. $\frac{1 - 3i}{5}$

E. None of the above

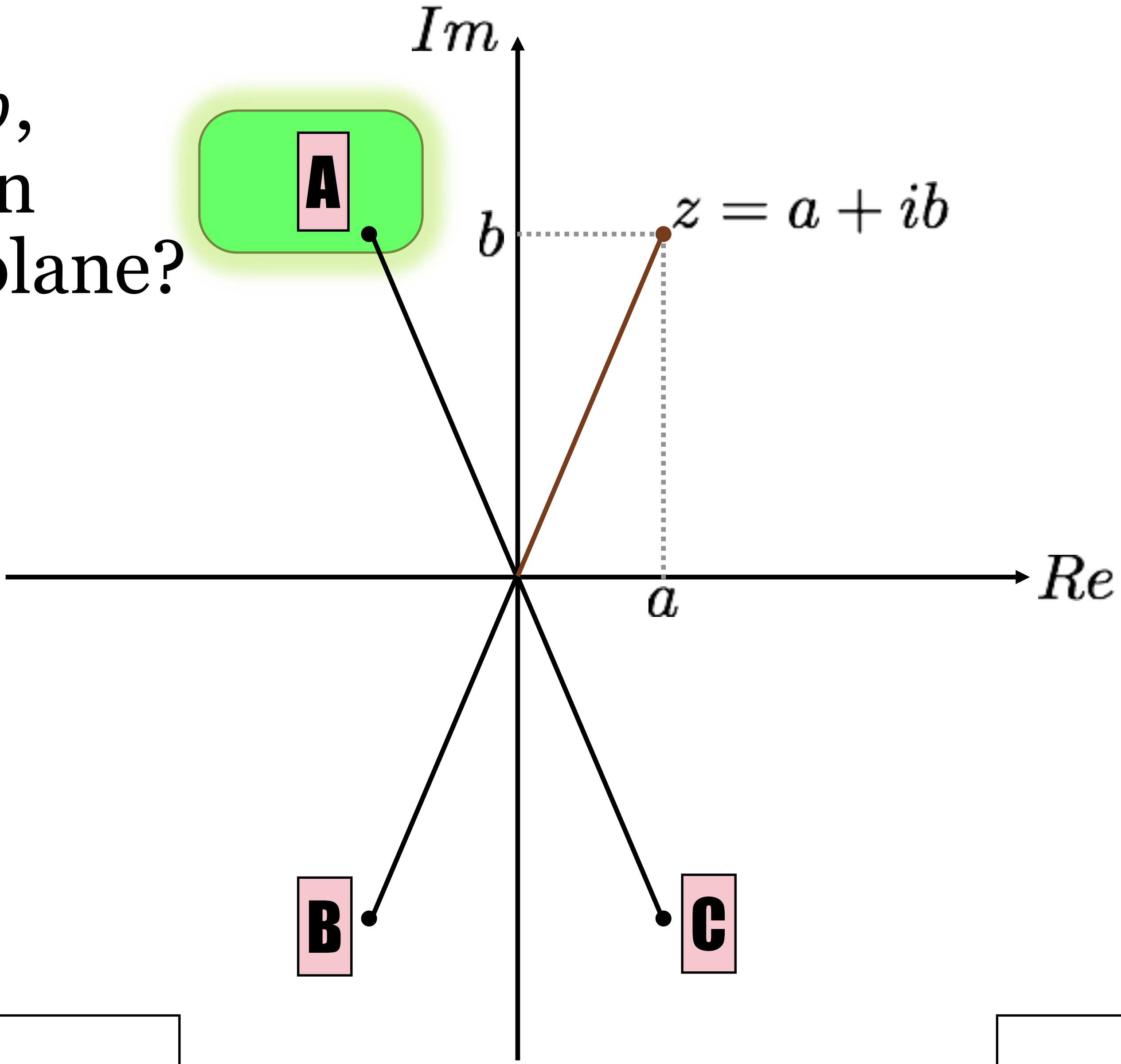
For $z = a + ib$, where is it's complex conjugate $\bar{z}$ on the complex plane?



D. Not enough information

E. None of the above

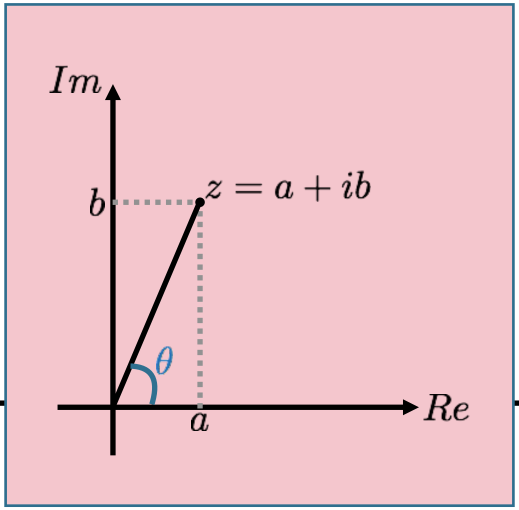
For $z = a + ib$, where is $-\bar{z}$ on the complex plane?



D.
Not enough information

E.
None of the above

What is $z = a + ib$ equivalent to?



A. $\sin\theta + i\cos\theta$

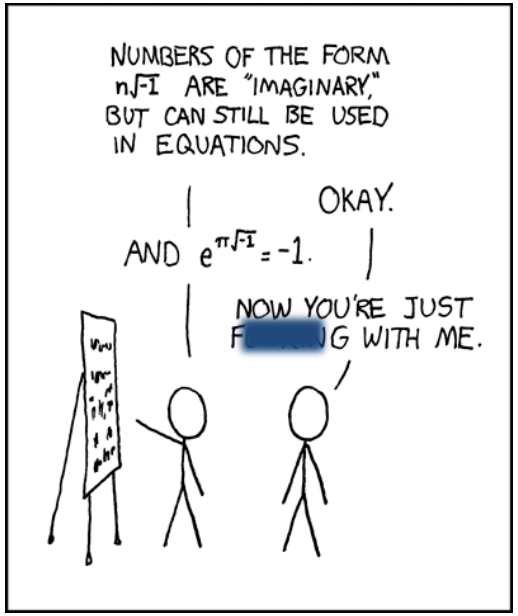
B. $\cos\theta + i\sin\theta$

C. $|z|(\cos\theta + i\sin\theta)$

D. $|z|(\sin\theta + i\cos\theta)$

E. $|z|(\cos\theta \times i\sin\theta)$

Polar Form

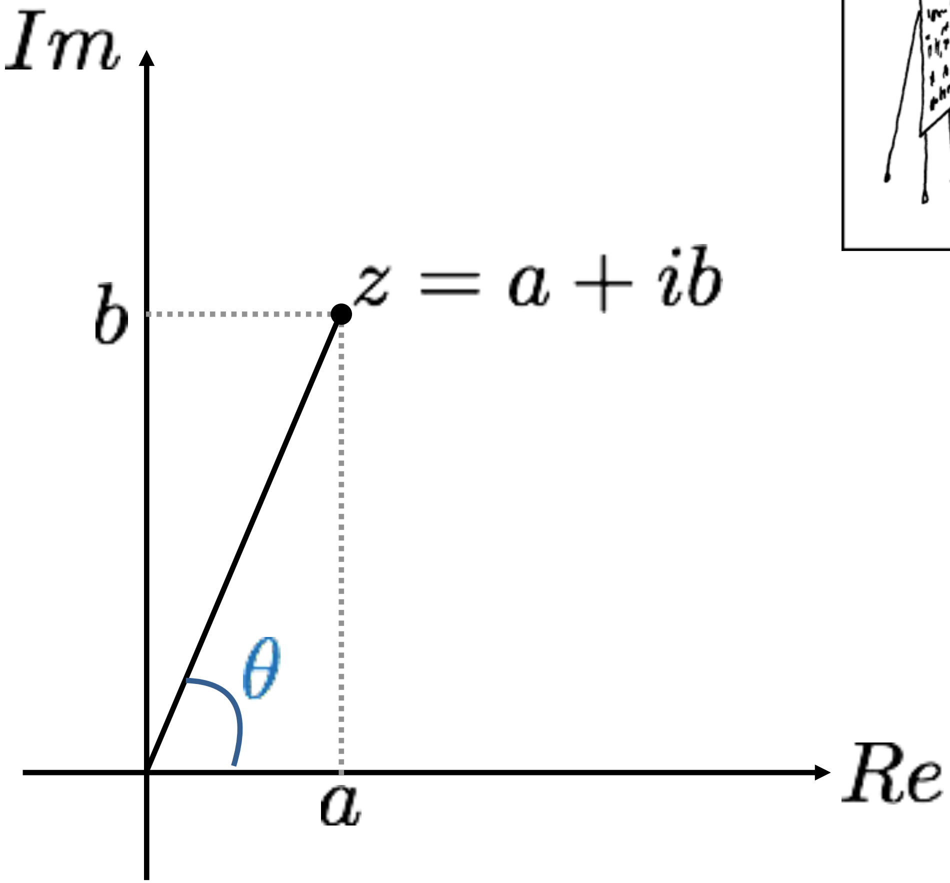


xkcd

Allows us to use all the nice features of exponentials in trig and wave problems

$$\frac{d}{dx}e^{iax} = iae^{iax}$$

$$e^{ix}e^{iy} = e^{i(x+y)}$$



Using the complex plane, we can re-express any complex number as:

$$z = a + ib = |z|(\cos\theta + i\sin\theta)$$

Using Euler's equation, we write this in **polar form** as

$$z = |z|(\cos\theta + i\sin\theta) = |z|e^{i\theta}$$

What is the complex conjugate $\bar{z}$ of $z = |z|e^{i\theta}$ in polar form?

A. $\bar{z} = |z|e^{i\theta}$

B. $\bar{z} = -|z|e^{i\theta}$

C. $\bar{z} = |z|e^{-i\theta}$

D. $\bar{z} = -|z|e^{-i\theta}$

E. None of the above

What is the inverse z^{-1} of $z = |z|e^{i\theta}$ in polar form?

A. $z^{-1} = \frac{1}{|z|}e^{i\theta}$

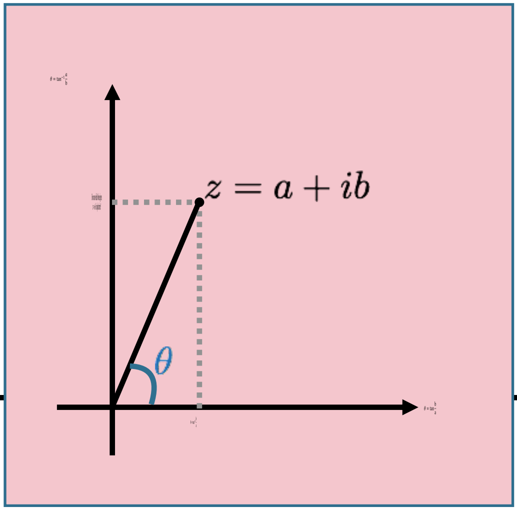
B. $z^{-1} = -\frac{1}{|z|}e^{i\theta}$

C. $z^{-1} = \frac{1}{|z|}e^{-i\theta}$

D. $z^{-1} = -\frac{1}{|z|}e^{-i\theta}$

E. None of the above

How can we find θ when given $z = a + ib$ in polar form?



A. $\theta = |z| \tan^{-1} \frac{a}{b}$

B. $\theta = \tan \frac{b}{a}$

C. $\theta = \tan \frac{a}{b}$

D. $\theta = \tan^{-1} \frac{a}{b}$

E. $\theta = \tan^{-1} \frac{b}{a}$

But always check for trig ambiguities!

$z = a + ib$ and $z = -a - ib$ give the same $tan^{-1} \frac{b}{a}$

Complex Numbers

Write the following in a+ib form and in polar form

$$\frac{i-\sqrt{3}}{1+i}$$

In a+ib form,

$$\frac{(1-\sqrt{3})+i(1+\sqrt{3})}{2}$$

In polar form,

$$\sqrt{2}e^{i\frac{7\pi}{12}}$$

Equivalent, which we can show as:

$$\frac{1}{2}(1-\sqrt{3}) = \sqrt{2}\cos\frac{7\pi}{12}$$

$$\frac{1}{2}(1+\sqrt{3}) = \sqrt{2}\sin\frac{7\pi}{12}$$

What is the polar form of $z = 2 - 2i$?

A. $z = 2\sqrt{2}e^{i\frac{\pi}{2}}$

B. $z = 2\sqrt{2}e^{i\frac{\pi}{4}}$

C. $z = -2\sqrt{2}e^{i\frac{3\pi}{4}}$

C: The same number, but not in pure polar form

D. $z = 2\sqrt{2}e^{-i\frac{\pi}{4}}$

E. None of the above

What is the polar form of $z = -2 - 2i$?

A. $z = 2\sqrt{2}e^{-i\frac{\pi}{4}}$

B. $z = 2\sqrt{2}e^{i\frac{\pi}{4}}$

Your calculator says B, but it's a lie!

C. $z = 2\sqrt{2}e^{i\frac{3\pi}{4}}$

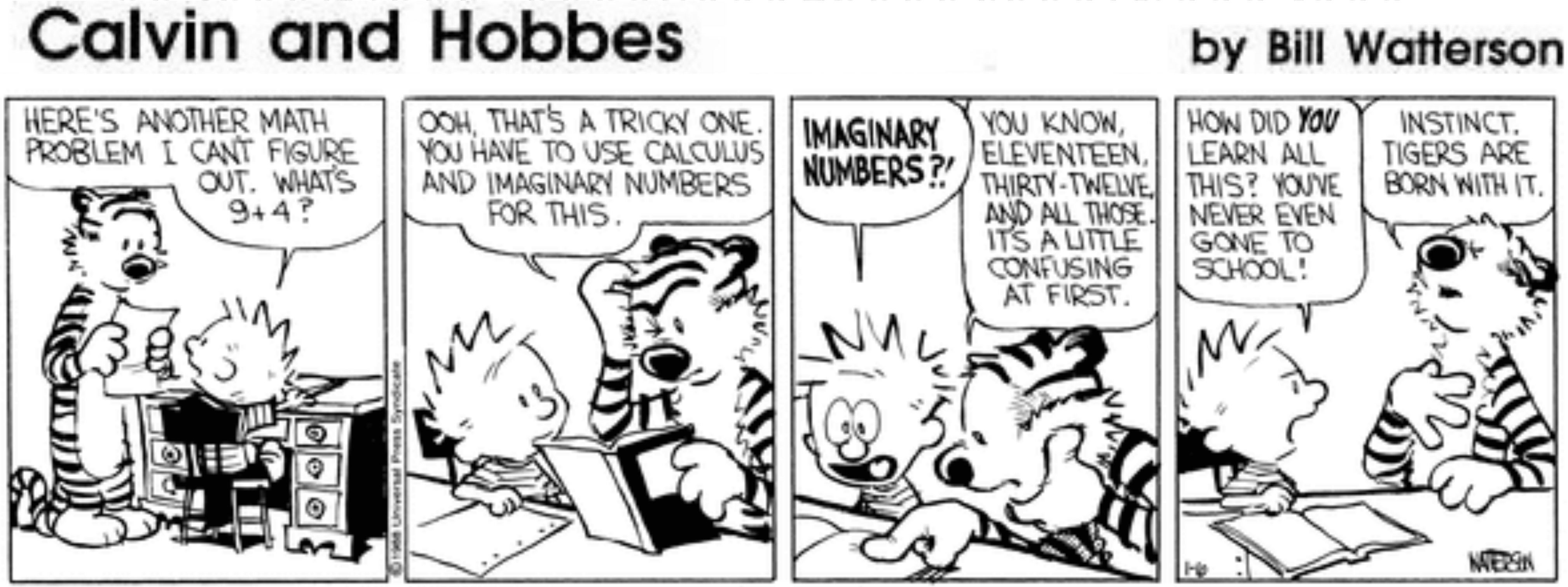
D. $z = 2\sqrt{2}e^{i\frac{5\pi}{4}}$

Is this unique?
Are there other options?

E. None of the above

$z = 2\sqrt{2}e^{-i\frac{3\pi}{4}}$

Now we're all tigers



...moving on

Question Break

VECTORS & LINEAR ALGEBRA

How confident do you feel working with **vectors and matrices?**

A. Linear algebra is easy!

B. I'm pretty confident

C. I'm starting to get used to it

D. Linear algebra is difficult

E. I'm completely lost

Vectors

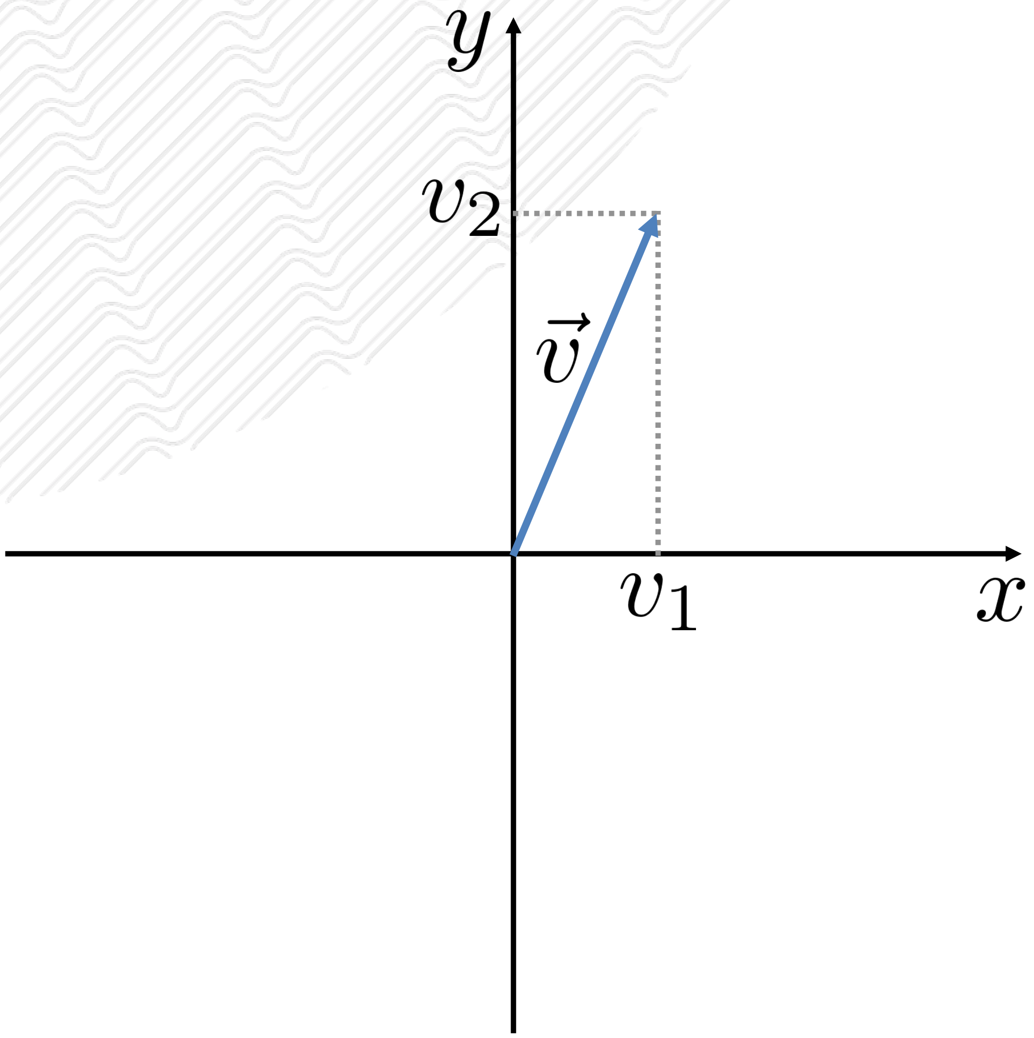
Vectors are an ordered set of numbers, mathematically.

In physics, we often interpret them as a number with direction

More abstractly, each entry is a distinguishable component

$$\vec{v} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} = v_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + v_2 \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

x-component y-component



Math with Vectors

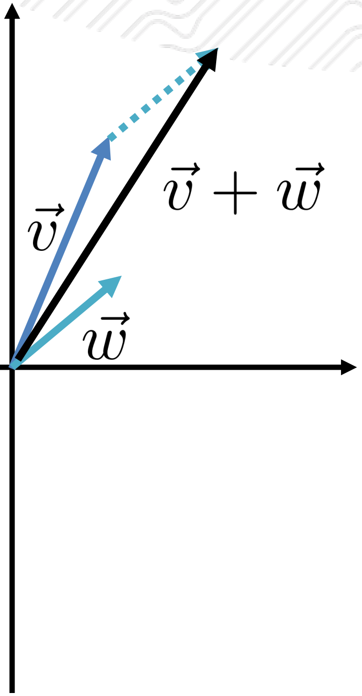
Vectors respect addition and scalar multiplication

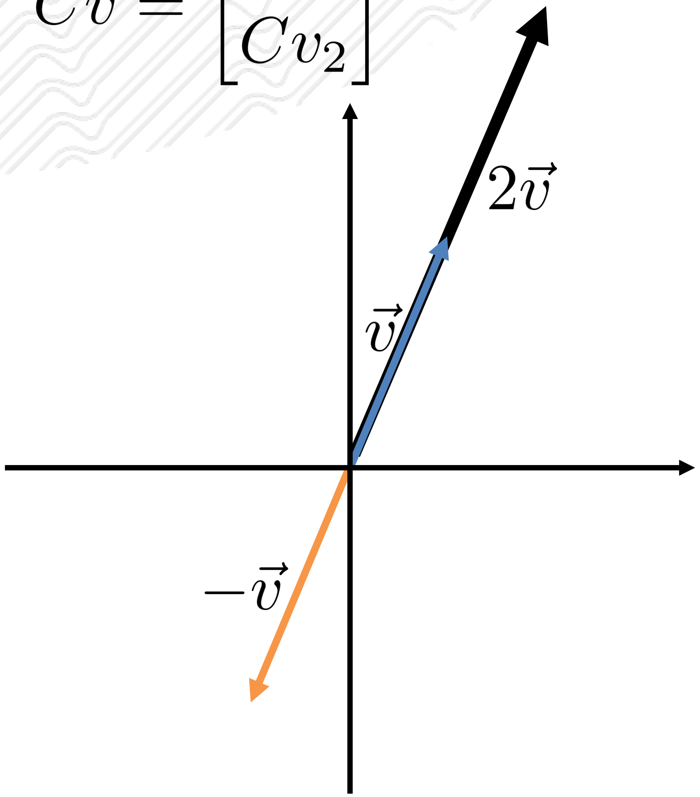
$$\vec{v} + \vec{w} = \begin{bmatrix} v_1 + w_1 \\ v_2 + w_2 \end{bmatrix}$$

$$C\vec{v} = \begin{bmatrix} Cv_1 \\ Cv_2 \end{bmatrix}$$

$$\vec{v} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}$$

$$\vec{w} = \begin{bmatrix} w_1 \\ w_2 \end{bmatrix}$$





What is $\begin{bmatrix} 4a \\ 6i \\ 2 \end{bmatrix} + \begin{bmatrix} 12b \\ \pi \\ \sin\theta \end{bmatrix}$

A. $\begin{bmatrix} 4a + 6i + 12b \\ 12b + \pi + \sin\theta \end{bmatrix}$

B. $\begin{bmatrix} 4a + 12b \\ \pi + 6i \\ 2 + \sin\theta \end{bmatrix}$

C. $\begin{bmatrix} 4a + 6i \\ 12b + \pi \\ 2 + \sin\theta \end{bmatrix}$

D. $4a + 12b + \pi + 2 + \sin\theta + 6i$

E. No answer exists

What is $\begin{bmatrix} 4a \\ 6i \\ 2 \end{bmatrix} + \begin{bmatrix} 12b \\ \pi \end{bmatrix}$

A. $\begin{bmatrix} 4a + 12b \\ \pi + 6i \end{bmatrix}$

B. $\begin{bmatrix} 4a + 12b \\ \pi + 6i \\ 2 \end{bmatrix}$

C. $\begin{bmatrix} 8a + 24b \\ 2\pi + 12i \end{bmatrix}$

D. $4a + 12b + \pi + 2 + 6i$

E. No answer exists

A Vector Glossary

$$\vec{v} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}$$

The **dimensionality** of a vector is the number of elements it has

$$\text{Dim}(\vec{v}) = 2 \times 1$$

The **absolute value** or **norm** of a vector is it's length

$$||\vec{v}||^2 = |v_1|^2 + |v_2|^2$$

A **unit vector** is a vector with a norm of 1

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

The **conjugate transpose** of a vector switches rows and columns and takes the complex conjugate of all elements

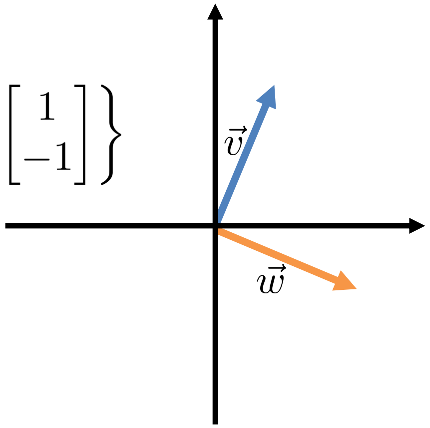
$$\vec{v}^\dagger = \begin{bmatrix} \bar{v}_1 & \bar{v}_2 \end{bmatrix}$$

The **dot** or **inner product** measures the projection of one vector onto another, and measures how alike two vectors are

$$\vec{v} \cdot \vec{w} = \vec{v}^\dagger \vec{w} = \sum_j \bar{v}_j w_j$$

Two perpendicular vectors have an inner product of zero, and are called **orthogonal**. If they are also unit vectors, they form an **orthonormal pair**

$$\left\{\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right\}, \left\{\frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix}\right\}$$



What is the inner product of $\vec{v} = \begin{bmatrix} 4a \\ 6i \\ 2 \end{bmatrix}, \quad \vec{w} = \begin{bmatrix} 12b \\ \pi \\ \sin\theta \end{bmatrix}$

A. $576ab\pi i \sin\theta$

B. $\begin{bmatrix} 4a + 12b \\ \pi + 6i \\ 2 + \sin\theta \end{bmatrix}$

C. $48ab - 6\pi i + 2\sin\theta$

D. $4a + 12b + \pi + 2 - 6i + \sin\theta$

E. No answer exists

What is the inner product of $\vec{v} = \begin{bmatrix} 2 \\ -1 \\ i \end{bmatrix}, \quad \vec{w} = \begin{bmatrix} i \\ 0 \\ 2 \end{bmatrix}$

A. 0 $\quad \vec{v} \cdot \vec{w} = \vec{v}^\dagger \vec{w} = \sum_j \bar{v}_j w_j$

B. $-1 + 4i$

C. $4i$

D. $\begin{bmatrix} 2i \\ 0 \\ 2i \end{bmatrix}$

E. No answer exists

Bases

A **basis** is an alphabet to make other vectors with

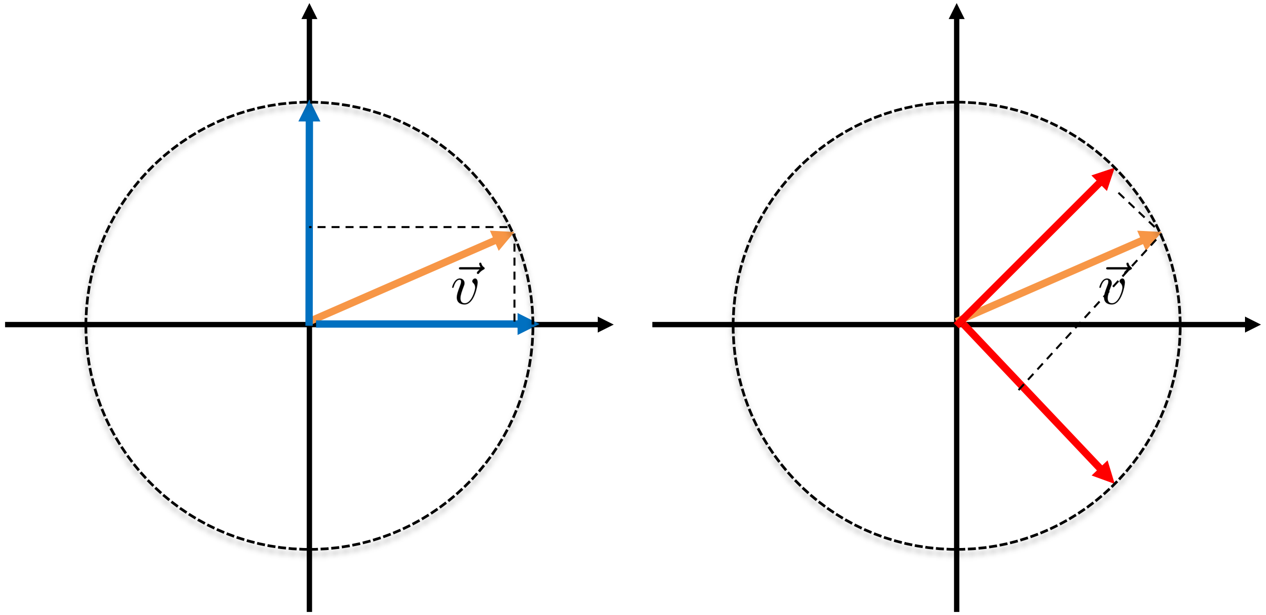
Any orthonormal pair forms an **orthonormal basis** in 2D, and any vector can be broken down into components in that basis

More generally, for *d* dimensions, any set of *d* linearly independent vectors form a basis

$$\hat{v}_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \hat{v}_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \hat{v}_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

$$\vec{v} = \begin{bmatrix} x \\ y \end{bmatrix} = x \begin{bmatrix} 1 \\ 0 \end{bmatrix} + y \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$= \frac{x+y}{\sqrt{2}} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} + \frac{x-y}{\sqrt{2}} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix}$$



Which set of vectors forms an **orthonormal** basis?

$$A = \left\{ \begin{bmatrix} 0 \\ 2 \end{bmatrix}, \begin{bmatrix} 2 \\ 0 \end{bmatrix} \right\} \qquad B = \left\{ \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\} \qquad C = \left\{ \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} -1 \\ 0 \end{bmatrix} \right\}$$

Not normalized!

Not orthogonal!

A. Only A

B. Only B

C. Only C

D. A and C

E. All are orthonormal bases

Which of the following vectors is **not** the same as the others?

A. $1 \times \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + 1 \times \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix} + 0 \times \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$

B. $0 \times \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} + 0 \times \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix} + \sqrt{2} \times \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$

C. $0 \times \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} - i \times \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ i \\ 1 \end{bmatrix} + 1 \times \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ i \end{bmatrix}$

D. $0 \times \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + \sqrt{2} \times \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} + 0 \times \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$

E. All are the same vector

Matrices

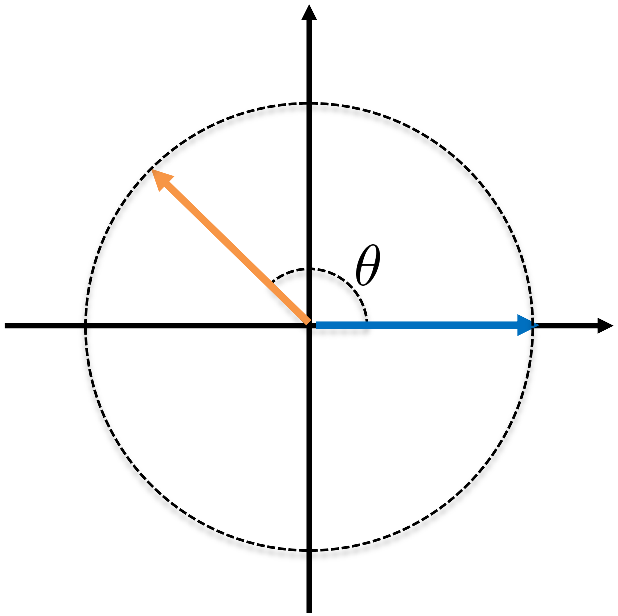
A **matrix** is a recipe for manipulating vectors

For example, the rotation matrix ***R*** rotates a vector

$$M\vec{v} = \begin{bmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \\ m_{41} & m_{42} & m_{43} \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix}$$

$$R = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

$$R\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \cos\theta \\ \sin\theta \end{bmatrix}$$



What is the size of this matrix?

$$M = \begin{bmatrix} 0 & 1 & -1 & 3 & -1 \\ 2 & -2 & 1 & 0 & 9 \\ 1 & 3 & 2 & 8 & -4 \end{bmatrix}$$

A. 3×5

B. 15

C. 5×3

D. 2×1

E. None of the above

Which addition is **not** allowed?

$$M = \begin{bmatrix} 0 & 1 & -1 & 3 \\ 2 & -2 & 1 & 0 \\ 1 & 3 & 2 & -4 \end{bmatrix} \quad N = \begin{bmatrix} 1 & 3 \\ -1 & 6 \\ 0 & 8 \\ 4 & 3 \end{bmatrix} \quad P = \begin{bmatrix} 5 & 4 & 3 \\ 2 & 1 & 0 \end{bmatrix}$$

A. $M + N$

B. $M + P$

C. $N + P$

D. $M + N + P$

E. None are allowed

Which multiplication is **not** allowed?

NM MN $P = \begin{bmatrix} 5 & 4 & 3 \\ 2 & 1 & 0 \end{bmatrix}$

A. PM

B. NM

C. NP

D. MN

E. None are allowed

What is $M \times N$? $M = \begin{bmatrix} 0 & 1 & -1 \\ 2 & -2 & 1 \\ 1 & 3 & 2 \end{bmatrix}$ $N = \begin{bmatrix} -2 & 1 \\ -1 & 3 \\ 1 & -1 \end{bmatrix}$

A. $\begin{bmatrix} 0 & 1 \\ -2 & -6 \\ 1 & -3 \end{bmatrix}$

B. $\begin{bmatrix} 0 & -2 & 1 \\ 1 & -6 & -3 \end{bmatrix}$

C. $\begin{bmatrix} -2 & -1 & -3 \\ 4 & -3 & 8 \end{bmatrix}$

D. $\begin{bmatrix} -2 & 4 \\ -1 & -5 \\ -3 & 8 \end{bmatrix}$

E. None of the above

What is $M \times N$?

$$M = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad N = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

A. $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

B. $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$

This is $N * M$
Matrix multiplication,
in general,
does not commute!

C. $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$

D. $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

E. None of the above

What is the transpose of M? $M = \begin{bmatrix} 0 & 1 & -1 & 3 & -1 \\ 2 & -2 & 1 & 0 & 9 \\ 1 & 3 & 2 & 8 & -4 \end{bmatrix}$

A. $M^T = \begin{bmatrix} 0 & 2 & 1 \\ 1 & -2 & 3 \\ -1 & 1 & 2 \\ 3 & 0 & 8 \\ -1 & 9 & -4 \end{bmatrix}$

B. $M^T = \begin{bmatrix} 0 & -2 & -1 \\ -1 & 2 & -3 \\ 1 & -1 & -2 \\ -3 & 0 & -8 \\ 1 & -9 & 4 \end{bmatrix}$

C. $M^T = \begin{bmatrix} 1 & 3 & 2 & 8 & -4 \\ 2 & -1 & 1 & 0 & 9 \\ 0 & 1 & -1 & 3 & -1 \end{bmatrix}$

D. $M^T = \begin{bmatrix} 0 & 2 & 1 \\ 1 & -2 & 3 \\ -1 & 1 & 2 \end{bmatrix}$

E. None of the above

What is the **conjugate** transpose of M?

$$M = \begin{bmatrix} 1 & 3i & 4 \\ 3-i & e^{i\frac{\pi}{6}} & 0 \\ -2i & 2+i & 1 \end{bmatrix}$$

A. $M^\dagger = \begin{bmatrix} 1 & -3i & 4 \\ 3+i & e^{-i\frac{\pi}{6}} & 0 \\ 2i & 2-i & 1 \end{bmatrix}$

B. $M^\dagger = \begin{bmatrix} 1 & 3-i & -2i \\ 3i & e^{i\frac{\pi}{6}} & 2+i \\ 4 & 0 & 1 \end{bmatrix}$

C. $M^\dagger = \begin{bmatrix} 1 & 3+i & 2i \\ -3i & e^{-i\frac{\pi}{6}} & 2-i \\ 4 & 0 & 1 \end{bmatrix}$

D. $M^\dagger = \begin{bmatrix} 1 & 3+i & 2i \\ -3i & e^{i\frac{\pi}{6}} & 2-i \\ 4 & 0 & 1 \end{bmatrix}$

E. None of the above

Eigenvectors

An **eigenvector** is a vector whose direction does not change after matrix multiplication.

$$M\vec{v} = k\vec{v}$$

Each matrix has its own set of eigenvectors.

$$\begin{bmatrix} \frac{1}{2} & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{2} \times \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} -2 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = 1 \times \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} -2 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ -1 \end{bmatrix} = -1 \times \begin{bmatrix} 0 \\ 1 \\ -1 \end{bmatrix}$$

Which is **not** an eigenvector of M?

$$M = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ 0 & -1 & 0 \\ \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{bmatrix}$$

A. $\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$

B. $\begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$

C. $\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ 0 & -1 & 0 \\ \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} \sqrt{2} \\ -1 \\ \sqrt{2} \end{bmatrix}$$

D. $\begin{bmatrix} 1 \\ 0 \\ -1 \end{bmatrix}$

E. None of the above

Question Break

THE POSTULATES OF QUANTUM MECHANICS

We have the ingredients,
let’s make a stew

The Postulates of Quantum Mechanics

States	1) Quantum states are described by **unit vectors** in complex, potentially **high-dimensional Hilbert spaces**.
Measurements	2) The probability of measuring a system in a given state is given by the **absolute-value-squared** of the **inner product** of the output state and the current state of the system. Immediately after the measurement, the wavefunction **collapses** into that state.
Processes	3) Valid quantum state **transformations** are given by **unitary** operations.
Systems	4) Separate quantum systems are described by the **tensor product** of the separate, individual Hilbert spaces.
Values	5) Physical **observables** are represented by the **eigenvalues** of Hermitian Operators on the Hilbert space.

Quantum States

A state describes <u>properties</u> of a system

Classical

A quantum state describes <u>properties</u> of a quantum system

Quantum

Specifics Tomorrow!

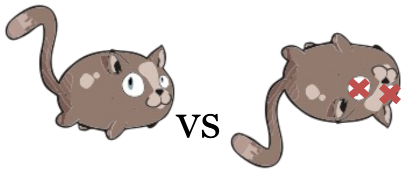
Energy State | Electron Spin | Circuit QED | Photon Polarization

Mutually Exclusive States

- Two states are mutually exclusive if they are:
  - Distinguishable and impossible to confuse
  - Cannot both occur at the same time

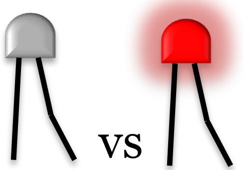
Classical

vs

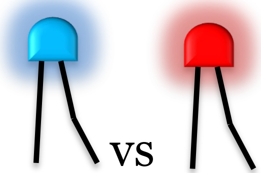


vs

0 vs 1



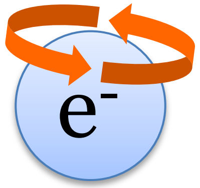
vs



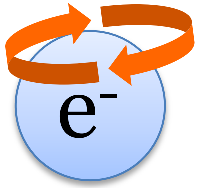
vs

Quantum

For example, consider electron spin



Can only take one of two values (⟳ or ⟲)



Which of the following are **NOT** mutually exclusive?

A. Heads *or* Tails on a coin

B. Wearing Red Socks *or* Wearing a Blue Shirt

Can do both at the same time

C. Being in Toronto *or* Being in Montreal

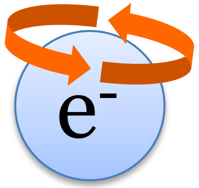
D. Having a Ball *or* Not Having a Ball

E. All of the above are mutually exclusive

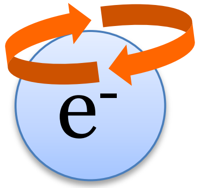
States as Vectors

1) Quantum states are described by **unit vectors** in complex, potentially **high-dimensional Hilbert spaces**.

Consider electron spin



Can only take one of two values



We'll represent them as a pair of orthogonal unit vectors

$$v_{\circlearrowleft} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad v_{\circlearrowright} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

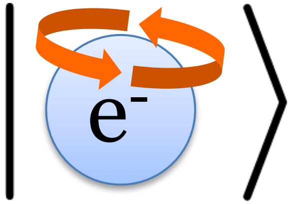
Why orthogonal?
They're impossible to confuse!
A ⟳ electron has no ⟲ component,
just like an x-vector has no y-component

States as Kets

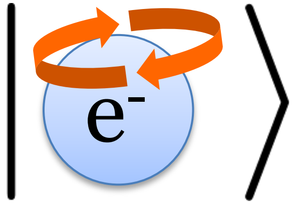
We call any two-dimensional quantum state a "qubit"

Qubit = Quantum Bit

We use a "ket" to denote a quantum state vector



$$:= |0\rangle$$



$$:= |1\rangle$$

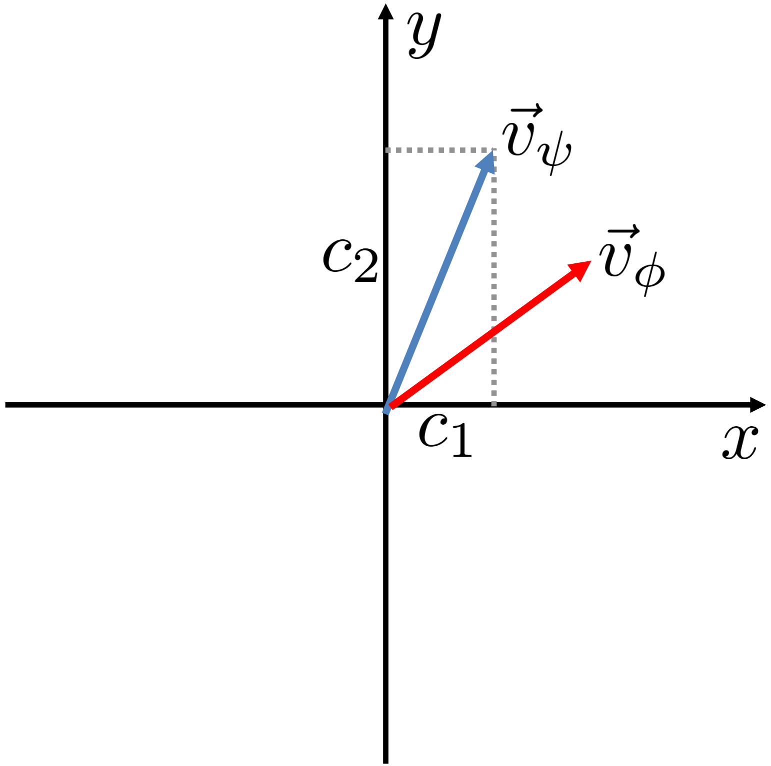
$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

We'll see this for numerous physical systems,
but the end result is always the same:
<u>Linear algebra is the rulebook for quantum mechanics</u>

States as Kets

$$|\psi\rangle = \vec{v}_\psi = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$$

A “ket” is a column vector



For now,
think of each component as how alike the state is to each of the mutually exclusive options.

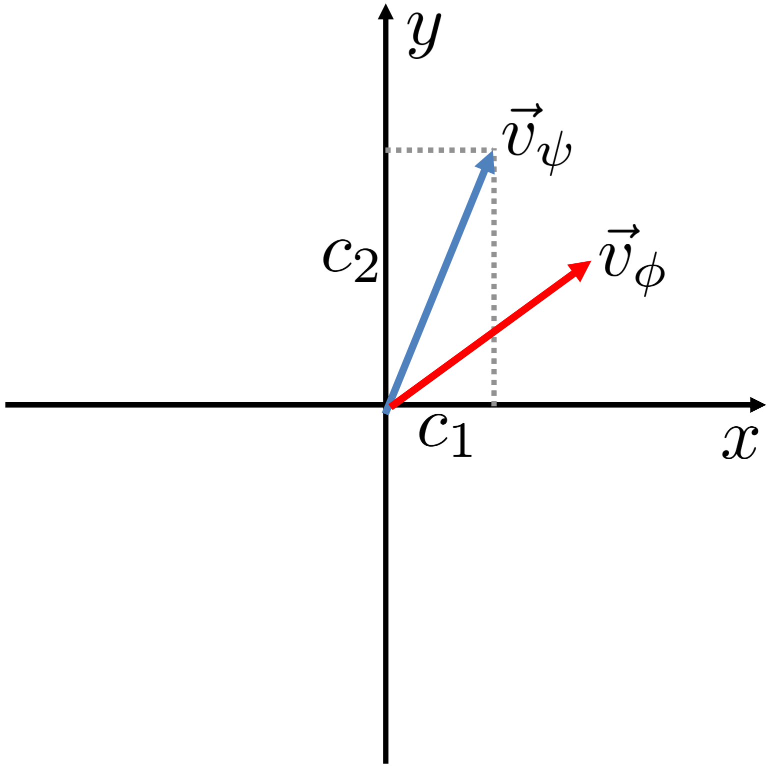
$$|\psi\rangle = \begin{bmatrix} 0.97 \\ 0.22 \end{bmatrix}$$ is more like $$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$|\psi\rangle = \begin{bmatrix} 0.26 \\ 0.96 \end{bmatrix}$$ is more like $$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Bra-Ket Notation

$$|\psi\rangle = \vec{v}_\psi = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$$

A "ket" is a column vector



$$\langle\psi| = \vec{v}_\psi^\dagger = \begin{bmatrix} \bar{c}_1 & \bar{c}_2 \end{bmatrix}$$

A "bra" is it's conjugate transpose
(row vector)

$$\langle\phi|\psi\rangle = \vec{v}_\phi^\dagger \vec{v}_\psi = \vec{v}_\phi \cdot \vec{v}_\psi$$

A bra and a ket together provides the inner product or overlap of the two states

Just like the inner product tells us how alike two vectors are, it will tell us how alike two quantum states are

Bra-Ket Notation

Why do we bother?

Extends to systems with more than two dimensions

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \text{ OR } \begin{bmatrix}1\\0\\0\end{bmatrix} \text{ OR } \begin{bmatrix}1\\0\\0\\0\end{bmatrix} \text{ OR } \begin{bmatrix}1\\0\\0\\0\\\vdots\end{bmatrix}$$

e.g. Electron with two possible spins and two possible energies
Photon with many possible positions

We can easily distinguish vectors, matrices, and numbers

Column Vector	$\|\psi\rangle$	$M\|\psi\rangle$
Row Vector	$\langle\psi\|$	$\langle\psi\|M^\dagger$
Scalar number	$\langle\phi\|\psi\rangle$	$\langle\phi\|A\|\psi\rangle$
Matrix	$\|\phi\rangle\langle\psi\|$	M

When the brakets are closed, we get a number out

What kind of mathematical object is this?

$$\langle \phi | M U_f M^\dagger | \psi \rangle \langle \gamma | H | \psi \rangle$$

A. A number

B. A matrix

C. A row vector

D. A column vector

E. None of the above

What kind of mathematical object is this?

$$|\phi\rangle\langle\psi|UXU^\dagger|\gamma\rangle$$

A. A number

B. A matrix

C. A row vector

D. A column vector

E. None of the above

Up next…

Test your knowledge!
Problem Sets #1/2 Available Now

- The history of quantum mechanics, from ancient Greece to laser beams
  - A Quantum History: this afternoon at 2:30 ET.
- Ask any questions about the problem set
  - Problem Solving Session after A Quantum History
- We'll talk and see how we use the linear algebra rulebook to describe real quantum experiments
  - Quantum Mechanics & Polarization: tomorrow at 10:30 ET.

Question Break

Quantum Measurement (aka Born's Rule)

The probability of measuring a system in a given state is given by the **absolute-value-squared** of the **inner product** of the output state and the current state of the system.

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

Is it "0" or "1"?

$$P(0) = |\langle 0|0\rangle|^2 = 1$$

$$P(1) = |\langle 1|0\rangle|^2 = 0$$

This is why a quantum state must be a **unit vector**, or else the probabilities would not add up to one.

Superposition

What about this state?

$$|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$$

It has both a “0” and a “1” component.

What does it mean?

Quantum Measurement

The probability of measuring a system in a given state is given by the **absolute-value-squared** of the **inner product** of the output state and the current state of the system.

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

Is it "0" or "1"?

$$P(0) = |\langle 0|0\rangle|^2 = 1$$

$$P(1) = |\langle 1|0\rangle|^2 = 0$$

$$|+\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

Is it "0" or "1"?

$$P(0) = |\langle 0|+\rangle|^2 = \frac{1}{2}$$

$$P(1) = |\langle 1|+\rangle|^2 = \frac{1}{2}$$

$$|+\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

Is it "+" or "-"?

$$P(+) = |\langle +|+\rangle|^2 = 1$$

$$P(-) = |\langle -|+\rangle|^2 = 0$$

Superposition Bases

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}}$$

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

$$|1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}}$$

What about superpositions of superpositions?

How do we interpret it?

Quantum Superposition

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

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

The particle is both
"0" AND "1"
at the same time

BUT

When measured in the 0/1 basis,
it will be found as
"0" OR "1"
<u>randomly</u>

<u>Measurement Basis</u>
Defines which "question"
I ask the particle

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}}$$

$$|1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}}$$

The particle is both
"+" AND "-"
at the same time

BUT

When measured in the +/- basis,
it will be found as
"+" OR "-"
<u>randomly</u>

Superposition Bases

Superposition basis
(X)

$$|+\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$$

$$|-\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$$

Computational basis
(Z)

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

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

Superposition basis
(Y)

$$|+_i\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\+i\end{bmatrix}$$

$$|-_i\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-i\end{bmatrix}$$

Generally, for qubits, we can form a basis with:

$$|\psi\rangle = \cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle$$

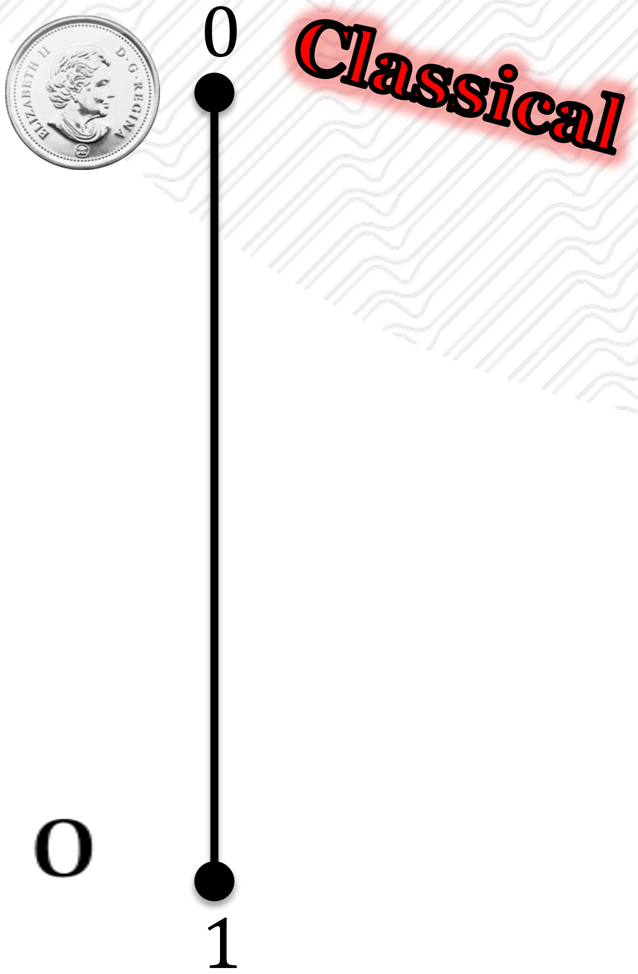
$$|\psi_\perp\rangle = \sin\theta|0\rangle - e^{i\phi}\cos\theta|1\rangle$$

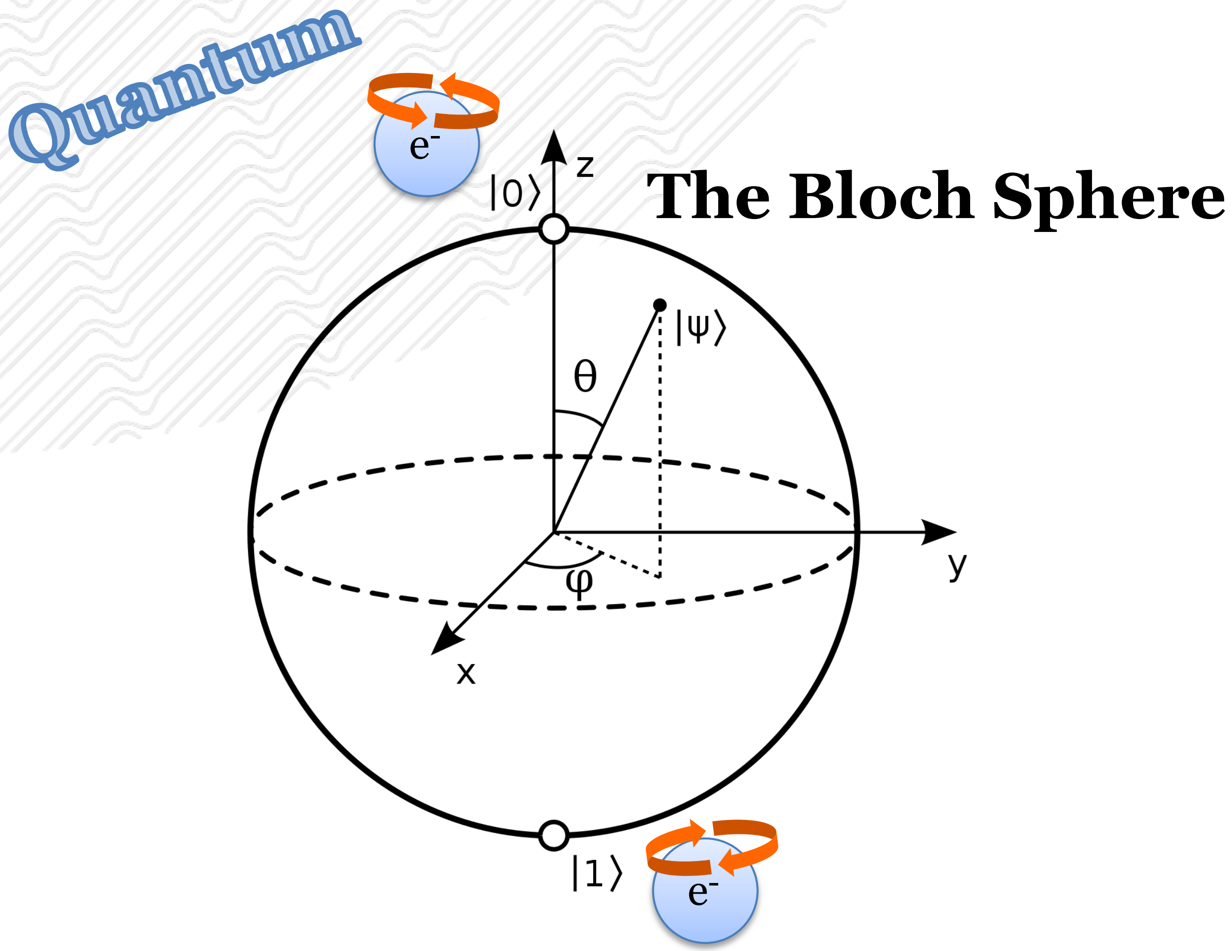
Measurement Bases

Z basis	X basis	Y basis
$\|0\rangle$	$\|0\rangle = \|+\rangle + \|-\rangle$	$\|0\rangle = \|+_i\rangle + \|-_i\rangle$
$\|1\rangle$	$\|1\rangle = \|+\rangle - \|-\rangle$	$\|1\rangle = \|+_i\rangle - \|-_i\rangle$
$\|+\rangle = \|0\rangle + \|1\rangle$	$\|+\rangle$	$\|+\rangle = \|+_i\rangle + i\|-_i\rangle$
$\|-\rangle = \|0\rangle - \|1\rangle$	$\|-\rangle$	$\|-\rangle = \|+_i\rangle - i\|-_i\rangle$
$\|+_i\rangle = \|0\rangle + i\|1\rangle$	$\|+_i\rangle = \|+\rangle + i\|-\rangle$	$\|+_i\rangle$
$\|-_i\rangle = \|0\rangle - i\|1\rangle$	$\|-_i\rangle = \|+\rangle - i\|-\rangle$	$\|-_i\rangle$

In quantum computing,
there are many different questions I can ask my qubits.

Quantum vs. Classical





$$\mathrm{VAL} = (\text{“0”})Pr(0) + (\text{“1”})Pr(1)$$

$$|\psi\rangle = \cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle$$

Question Break

Collapse

Immediately after the measurement,
the wavefunction collapses into that state

What's the probability of finding $|+\rangle$ in the state $|0\rangle$?

$$|\langle 0|+\rangle|^2 = \frac{1}{2}$$

What's the state after finding $|+\rangle$ in the state $|0\rangle$?

$$|0\rangle$$

Will be a major focus in tomorrow's discussion

What's the probability of finding $|\psi\rangle$ in the state $|+_i\rangle$?

$$|\psi\rangle = \cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle$$

Transformations

Valid quantum state **transformations** are given by **unitary** operations.

$$||U\vec{v}|| = ||\vec{v}||$$

$$U^\dagger U = U U^\dagger = \mathbb{1}$$

These are the operations which make sure that quantum states remain valid quantum states.

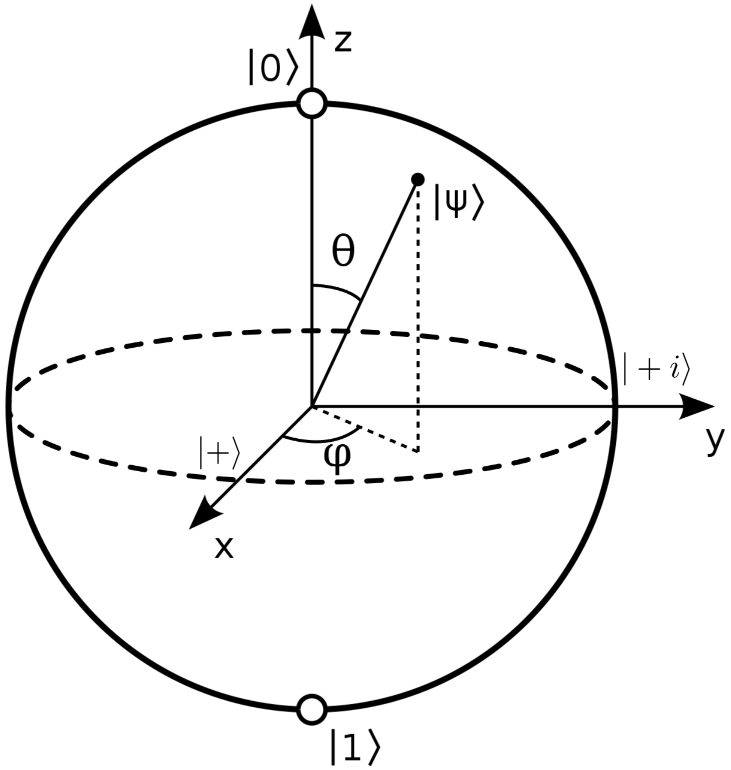
$$\langle\psi|U^\dagger U|\psi\rangle = \langle\psi|\psi\rangle$$

Maintains normalization

$$\langle\phi|U^\dagger U|\psi\rangle = \langle\phi|\psi\rangle$$

Maintains the inner product

Transformations



$$|\psi\rangle = \cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle$$

$$\langle\phi|U^\dagger U|\psi\rangle = \langle\phi|\psi\rangle$$

- Can be considered as rotations in the Bloch sphere
- Any two orthogonal states remain orthogonal
- Any non-orthogonal states remain non-orthogonal

Matrices in Bra-Ket Notation

$$\mathbb{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

The identity matrix
a.k.a. the do-nothing transformation

$$\begin{aligned} \mathbb{1} &= |0\rangle\langle 0| + |1\rangle\langle 1| \\ &= |+\rangle\langle +| + |-\rangle\langle -| \end{aligned}$$

In bra-ket notation,
we can see that it takes
each state back to itself,
thus doing *nothing* effectively.

This holds for any orthonormal basis.

$$\text{If} \quad M = |+\rangle\langle +_i| + |-\rangle\langle -_i|$$

What is $M|-_i\rangle$?

A. $|+\rangle$

B. $|-\rangle$

C. $|+i\rangle$

D. $|-i\rangle$

E. $|0\rangle$

Matrices in Bra-Ket Notation

NOT: $$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0| = |+\rangle\langle +| - |-\rangle\langle -|$$

Same effect
in a different basis

PHASE: $$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1| = |+\rangle\langle -| + |-\rangle\langle +|$$

Matrices in Bra-Ket Notation

$H|0\rangle?$ $H|1\rangle?$

$H|+\rangle?$ $H|-\rangle?$

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$
$$= |+\rangle\langle 0| + |-\rangle\langle 1|$$
$$= |0\rangle\langle +| + |1\rangle\langle -|$$

We can construct
any change of basis
this way!

$$|0\rangle\langle\psi| + |1\rangle\langle\psi_\perp|$$

Be sure that the bras and kets
both contain
an entire orthonormal basis
to ensure unitarity!

A quantum coin flip

Changes basis from Z to X and back again

A perfect example of a *change-of-basis* operation

Question Break

Composite Quantum Systems

Separate quantum systems are described by the **tensor product** of the separate, individual Hilbert spaces.

Alice's Qubit

$$|0\rangle_A$$

Alice & Bob's Two-Qubit System

$$|0\rangle_A \otimes |1\rangle_B = |01\rangle$$

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

Bob's Qubit

$$|1\rangle_B$$

Composite Quantum Systems

Alice & Bob's Two-Qubit System

$$|\psi\rangle_A \otimes |\phi\rangle_B = |\Psi\rangle_{AB}$$

More details when discussing entanglement this Friday!

New Computational Basis

$$|00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \qquad |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$|10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \qquad |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Composite Systems

We can use bra-ket notation to simplify composite system problems.

Find the state
in the computational basis

$$|+\rangle_A \otimes |-\rangle_B$$

$$\frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}$$

More details when discussing entanglement this Friday!

Observables

Physical **observables** are represented by the eigenvalues of **Hermitian operators** on the Hilbert space.

Essentially, while complex numbers and vectors are important for calculation, when we measure something in the lab, we get a **real number** out

A Hermitian operator is it's own conjugate transpose

$$A = A^\dagger$$

Basically the matrix equivalent of a "real number"

Implies that all of its eigenvalues are real numbers

Observables

We observe if an electron is in the ground state or the excited state

We assign different energies E to each state

$$A = (E_g) \times |g\rangle\langle g| + (E_e) \times |e\rangle\langle e|$$

Expected (average) value of the observable for different quantum states:

$$\langle g|A|g\rangle = E_g$$
$$\langle e|A|e\rangle = E_e$$

$$\langle +|A|+\rangle = \boxed{?}$$

The Postulates of Quantum Mechanics

$$|\langle\psi|\psi\rangle|^2 = 1$$

1) Quantum states are described by **unit vectors** in complex, potentially **high-dimensional Hilbert spaces**.

$$P(\phi) = |\langle\phi|\psi\rangle|^2$$

2) The probability of measuring a system in a given state is given by the **absolute-value-squared** of the **inner product** of the output state and the current state of the system. Immediately after the measurement, the wavefunction **collapses** into that state.

$$|\psi\rangle_1 = U_1|\psi\rangle_0$$

3) Valid quantum state **transformations** are given by **unitary** operations.

$$|\Psi\rangle_{AB} = |\psi\rangle_A \otimes |\phi\rangle_B$$

4) Separate quantum systems are described by the **tensor product** of the separate, individual Hilbert spaces.

$$\langle A\rangle = \langle\psi|A|\psi\rangle$$

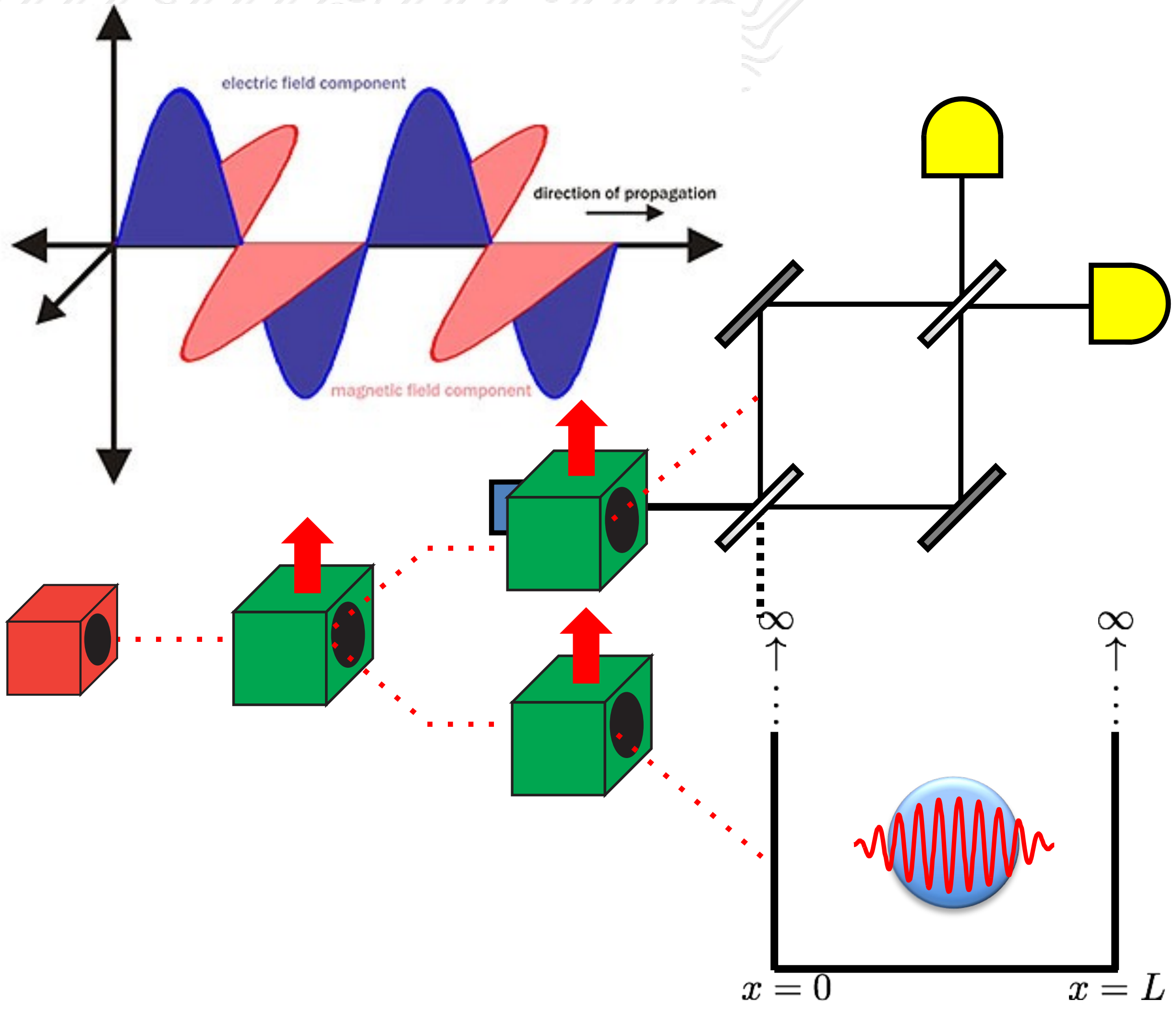
5) Physical **observables** are represented by the **eigenvalues** of Hermitian Operators on the Hilbert space.

But is it real?

Linear algebra is the
rulebook
for quantum mechanics

It is only useful insofar
as it predicts what happens
in real experiments

Tomorrow…



Composite Operations

What if Alice and Bob perform unitary transformations on their states?

Alice's Qubit

$$U|\psi\rangle_A$$

Alice & Bob's Two-Qubit System

$$U|\psi\rangle_A \otimes V|\phi\rangle_B$$

$$= (U \otimes V)(|\psi\rangle_A \otimes |\phi\rangle_B)$$

Bob's Qubit

$$V|\phi\rangle_B$$

$$U \otimes V = \begin{bmatrix} u_1v_1 & u_1v_2 & u_2v_1 & u_2v_2 \\ u_1v_3 & u_1v_4 & u_2v_3 & u_2v_4 \\ u_3v_1 & u_3v_2 & u_4v_1 & u_4v_2 \\ u_3v_3 & u_3v_4 & u_4v_3 & u_4v_4 \end{bmatrix} = \begin{bmatrix} u_1V & u_2V \\ u_3V & u_4V \end{bmatrix}$$

Composite Systems

We can use bra-ket notation to simplify composite system problems.

Find the state in the computational basis

$$|+\rangle_A \otimes |-\rangle_B$$

Find the matrix

$$Z_A \otimes Z_B$$

$$\frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}$$

$$|00\rangle\langle 00| - |01\rangle\langle 01| - |10\rangle\langle 10| + |11\rangle\langle 11|$$

More details when discussing entanglement this Friday!