Introduction to Quantum Information Science

Michael A. Nielsen

University of Queensland

What you don't need: quantum mechanics, computer science, or information theory.

What you do need: elementary linear algebra, mathematical maturity of a beginning grad student.

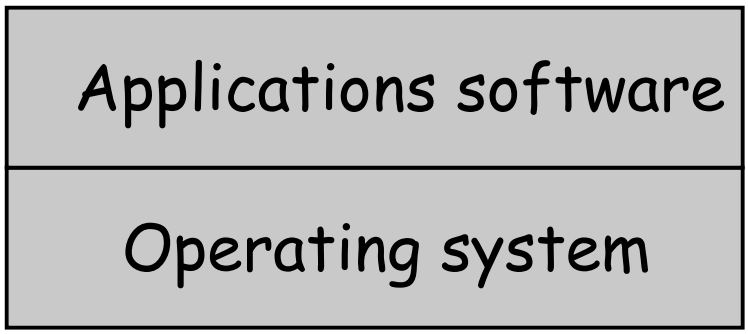
Rough Guide

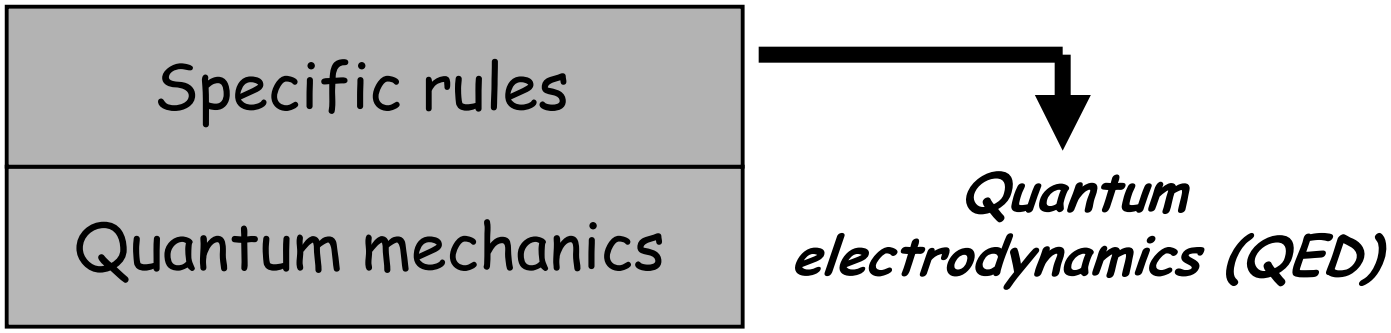
Lecture 1: Principles of quantum mechanics.
Lecture 2: Intro to quantum computation.
Lecture 3: Intro to quantum information.

What is quantum mechanics?

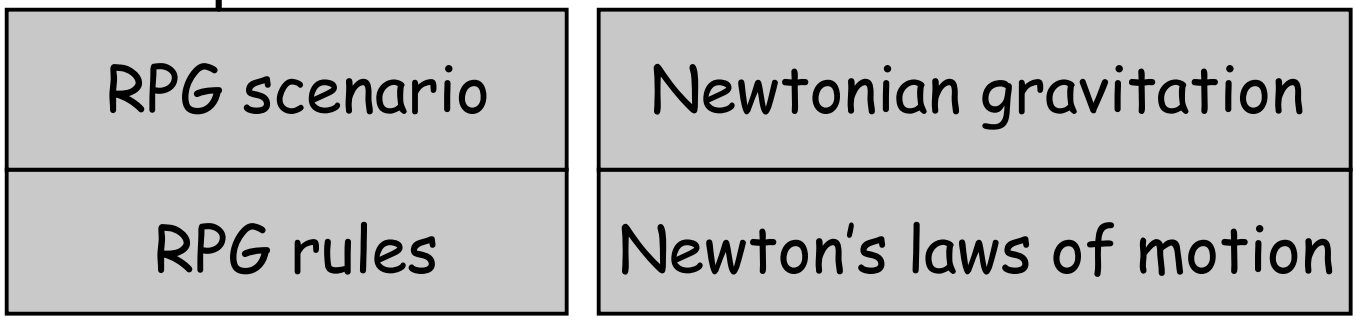
It is a ***framework*** for the development of physical theories.

It is ***not*** a complete physical theory in its own right.





QM consists of four mathematical postulates which lay the ground rules for our description of the world.



How successful is quantum mechanics?

It is ***unbelievably*** successful.

Critical for answering questions like:

Why do stars shine?

How was the Universe formed?

What is the chemical structure of DNA?

Why is matter stable?

No deviations from quantum mechanics are known

Most physicists believe that any "theory of everything" will be a quantum mechanical theory

Two clouds:

Conceptual issues (the "measurement problem") remain to be clarified.

Attempts to unify gravitation and quantum mechanics have failed.

"I ain't no physicist but I know what matters"
- Popeye the Sailor

The structure of quantum mechanics

linear algebra

Dirac notation

4 postulates of quantum mechanics

1. How to describe quantum states of a closed system.

"state vectors" and "state space"

2. How to describe quantum dynamics "unitary evolution"

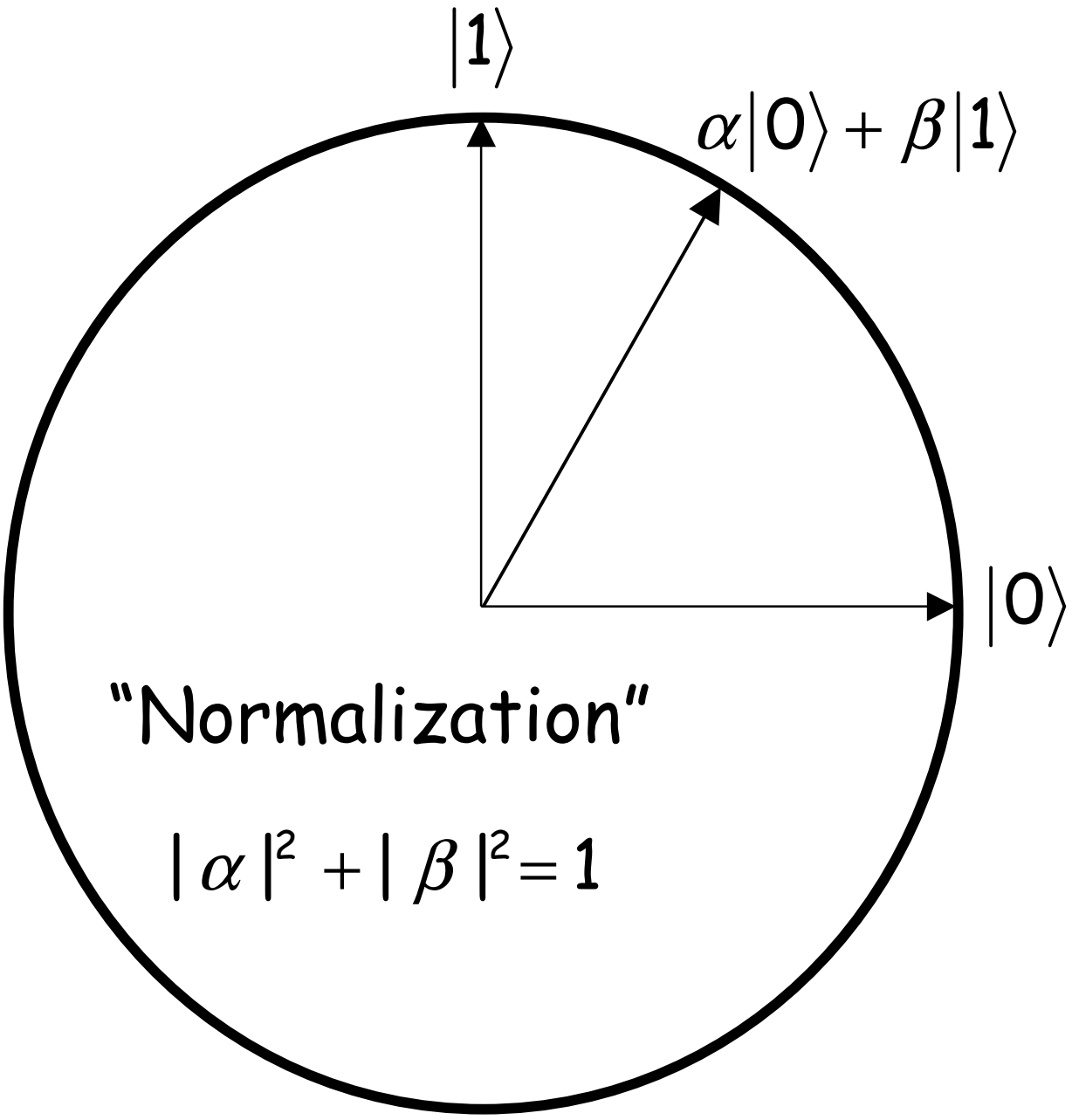
3. How to describe measurements of a quantum system.

"projective measurements"

4. How to describe quantum state of a composite system.

"tensor products"

Example: qubits (two level quantum systems)



$|0\rangle$ and $|1\rangle$ are the

computational basis states

Postulate 1: Rough Form

Associated to any closed quantum system is a complex vector space known as state space.

The state of a closed quantum system is a unit vector in state space.

Quantum mechanics does not prescribe the state spaces of specific systems, such as electrons. That's the job of a theory like quantum electrodynamics.

Example: we'll work mainly with qubits, which have state space $\boldsymbol{C}^2$.

$$\alpha|0\rangle + \beta|1\rangle \equiv \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

A few conventions

We write vectors in state space as:

$$|\psi\rangle$$

This type of notation is known as a ket.

We always assume that our physical systems have finite dimensional state spaces.

$$\boldsymbol{C}^{d}$$

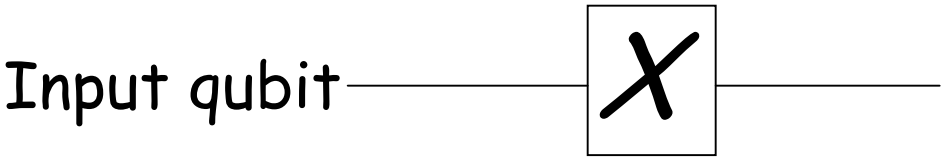
$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle + \ldots + \alpha_{d-1}|d-1\rangle$$

$$= \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{d-1} \end{bmatrix}$$

Qudit

Dynamics: quantum logic gates

Quantum not gate:



$$X|0\rangle = |1\rangle; \quad X|1\rangle = |0\rangle.$$

$$\alpha|0\rangle + \beta|1\rangle \rightarrow ?$$

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

Matrix representation:

$$X = \begin{array}{c} \\ |0\rangle \\ |1\rangle \end{array} \begin{array}{c} \begin{array}{cc} |0\rangle & |1\rangle \end{array} \\ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \end{array}$$

General quantum logic gate can be represented as a unitary matrix.

Unitary matrices

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Hermitian conjugation;
taking the adjoint

$$A^\dagger = \left(A^*\right)^T = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix}$$

A is said to be unitary if

$$AA^\dagger = A^\dagger A = I$$

We usually write unitary matrices as U.

Example:

$$XX^\dagger = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

Nomenclature tips

matrix

=

(linear) operator

=

(linear) transformation

=

(linear) map

=

gate

Postulate 2

The evolution of a closed quantum system is described by a unitary transformation.

$$|\psi'\rangle = U|\psi\rangle$$

Why unitaries?

Unitary maps are the only linear maps that preserve normalization.

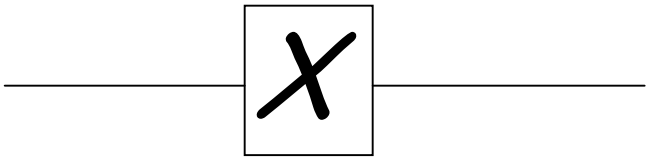
$$|\psi'\rangle = U|\psi\rangle$$

implies $\||\psi'\rangle| = |U|\psi\rangle| = \||\psi\rangle| = 1$

Exercise: prove that unitary evolution preserves normalization.

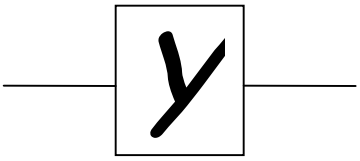
Pauli gates

X gate (AKA σ_x or σ_1)



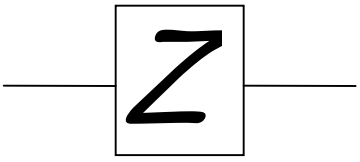
$$X|0\rangle = |1\rangle; \quad X|1\rangle = |0\rangle; \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Y gate (AKA σ_y or σ_2)



$$Y|0\rangle = i|1\rangle; \quad Y|1\rangle = -i|0\rangle; \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

Z gate (AKA σ_z or σ_3)



$$Z|0\rangle = |0\rangle; \quad Z|1\rangle = -|1\rangle; \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Notation: $\sigma_0 \equiv I$

Exercise: prove that $XY=iZ$

Exercise: prove that
$X^2=Y^2=Z^2=I$

Measuring a qubit: a rough and ready prescription

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

Quantum mechanics DOES NOT allow us to determine α and β, in general.

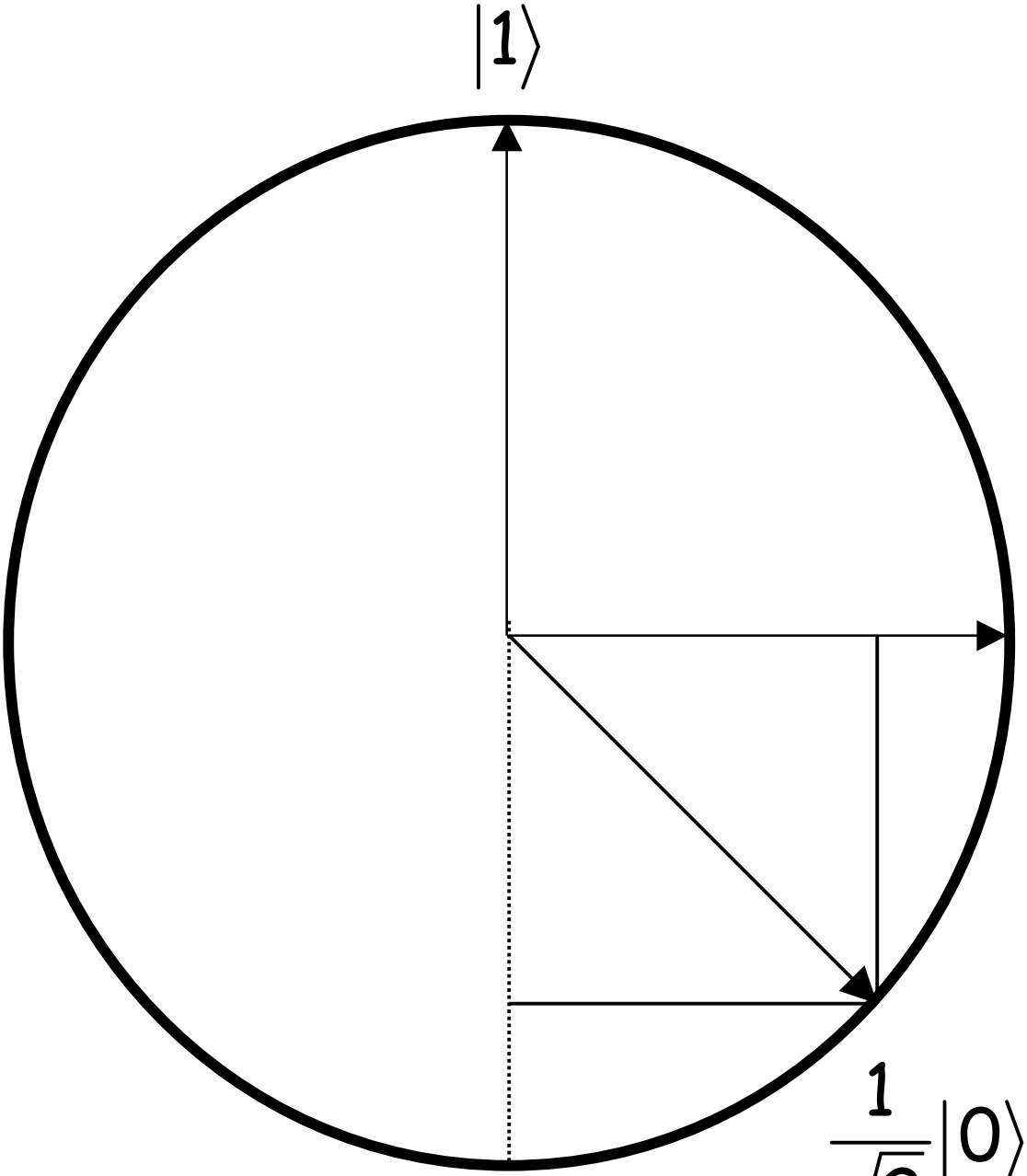
We can, however, read out some limited information about α and β.

"Measuring in the computational basis"

$$P(0) = |\alpha|^2; \qquad P(1) = |\beta|^2$$

Measurement unavoidably disturbs the system, leaving it in a state $|0\rangle$ or $|1\rangle$ determined by the outcome.

Measuring a qubit



$$P(0) = P(1) = \frac{1}{2}$$

More general measurements

Let $|e_1\rangle,\ldots,|e_d\rangle$ be an orthonormal basis for C^d.

A measurement of $|\psi\rangle$ in the basis $|e_1\rangle,\ldots,|e_d\rangle$ gives result j with probability

$$P(j) = \left\| |e_j\rangle \bullet |\psi\rangle \right|^2 .$$

Reminder:

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \bullet \begin{bmatrix} \chi \\ \delta \end{bmatrix} \equiv \alpha^* \chi + \beta^* \delta$$

Example

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

Introduce orthonormal basis

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

Observe that

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

$$|\psi\rangle = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle$$

Measuring in the $|+\rangle, |-\rangle$ basis gives

$$P(+) = \frac{|\alpha+\beta|^2}{2}; \qquad P(-) = \frac{|\alpha-\beta|^2}{2}$$

"Young man, in mathematics you don't understand things, you just get used to them." - John von Neumann

Inner products and duals

The inner product is used to define the dual of a vector $|\psi\rangle$.

If $|\psi\rangle$ lives in $\mathcal{C}^d$ then the dual of $|\psi\rangle$ is a function $\langle\psi|:\mathcal{C}^d \to \mathcal{C}$ defined by

$$\langle\psi|(|\phi\rangle) \equiv |\psi\rangle \bullet |\phi\rangle$$

Simplified notation: $\langle\psi|\phi\rangle$

Example

$$\langle 0|(\alpha|0\rangle + \beta|1\rangle) = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \bullet \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha$$

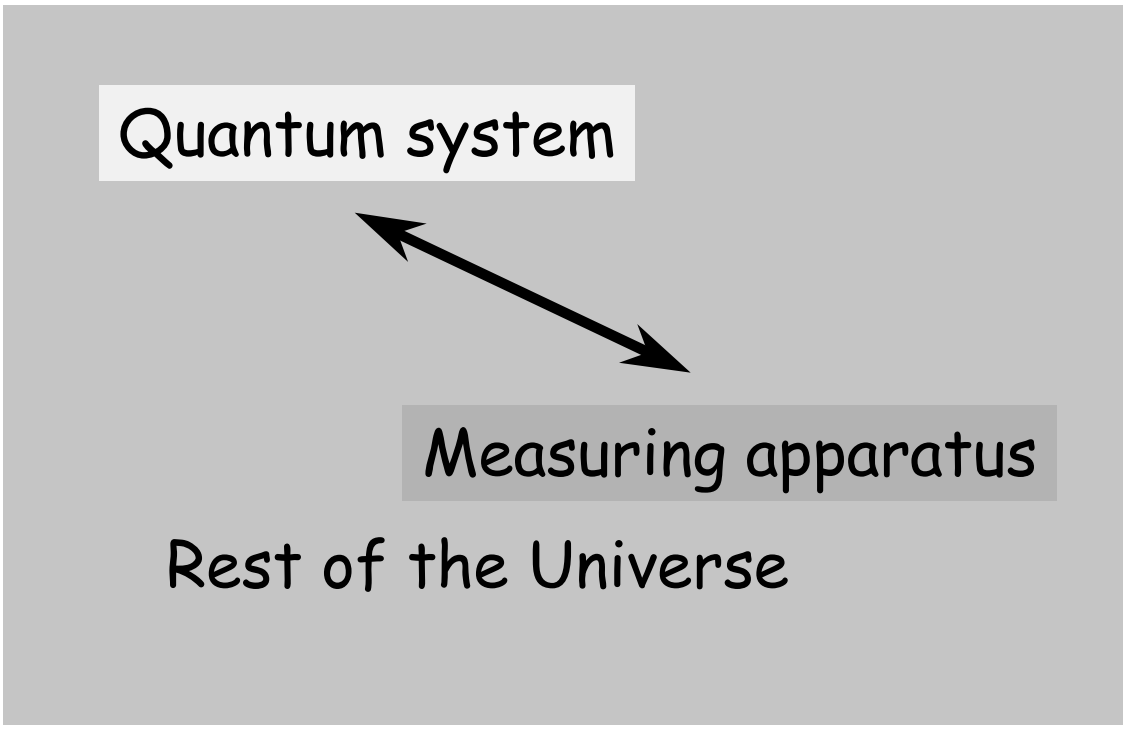
Postulate 3: rough form

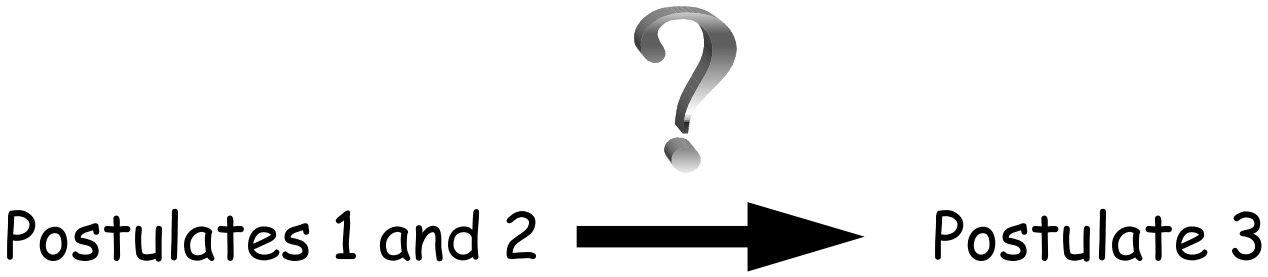
If we measure $|\psi\rangle$ in an orthonormal basis $|e_1\rangle,\ldots,|e_d\rangle$, then we obtain the result j with probability

$$P(j) = \left|\langle e_j|\psi\rangle\right|^2 .$$

The measurement disturbs the system, leaving it in a state $|e_j\rangle$ determined by the outcome.

The measurement problem





Exercise: solve the measurement problem.

Revised postulate 1

Associated to any closed quantum system is a complex inner product space known as state space.

The state of a closed quantum system is a unit vector in state space.

Note: These inner product spaces are often called Hilbert spaces.

Multiple qubit systems

"Hilbert space is a big place"
- Carlton Caves

$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

Measure: $P(x,y) = |\alpha_{xy}|^2$

General: $\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$

Classically, requires $O(2^n)$ bits to describe the state.

Postulate 4

The state space of a composite physical system is the tensor product of the state spaces of the component systems.

Example

Two qubit state space is

$$\mathcal{C}^2 \otimes \mathcal{C}^2 = \mathcal{C}^4$$

Notation for computational basis states:

$$|0\rangle \otimes |0\rangle;\ |0\rangle \otimes |1\rangle;\ |1\rangle \otimes |0\rangle;\ |1\rangle \otimes |1\rangle$$

Alternative notations:

$$|0\rangle|0\rangle;\ |0,0\rangle;\ |00\rangle.$$

Properties

$$z\left(|v\rangle \otimes |w\rangle\right) = \left(z|v\rangle\right) \otimes |w\rangle = |v\rangle \otimes \left(z|w\rangle\right)$$

$$\left(|v_1\rangle + |v_2\rangle\right) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$$

$$|v\rangle \otimes \left(|w_1\rangle + |w_2\rangle\right) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$$

Summary

Postulate 1: A closed quantum system is described by a unit vector in a complex inner product space known as state space.

Postulate 2: The evolution of a closed quantum system is described by a unitary transformation. $|\psi'\rangle = U|\psi\rangle$

Postulate 3: If we measure $|\psi\rangle$ in an orthonormal basis $|e_1\rangle,\ldots,|e_d\rangle$, then we obtain the result j with probability $P(j) = \left|\langle e_j|\psi\rangle\right|^2$.

The measurement disturbs the system, leaving it in a state $|e_j\rangle$ determined by the outcome.

Postulate 4: The state space of a composite physical system is the tensor product of the state spaces of the component systems.