Lecture 1: Quantum Mechanic – Resurrection

Quantum mechanics

Physicists have figured out a model which describes tiny physical systems perfectly: Quantum mechanics.

There's no need for you to understand the physics — if you're ready to just blindly believe the physicists. 😉

For us, quantum mechanics will simply be a set of mathematical "postulates": Stuff that you assume is true, not unlike axioms.

Quantum mechanics: Pure states

Postulate 1: States.
For every closed quantum mechanical system, there is a Hilbert space whose norm-1 vectors are exactly the set of states that the system can take on.

Remarks

1. "Closed" means: no information goes to the rest of the universe.
2. Occasionally you don't know what the Hilbert space is!
3. Terminology: "*state*" == "*norm-1 vector in a Hilbert space*"

Unicode: `Mathematical Right Angle Bracket`

LaTeX: `\rangle`

Notations:

- Hilbert space $\mathscr{A}, \mathscr{B}, \mathscr{H}$
- Vectors of Hilbert space: $|\mathrm{cat}\rangle = |\mathrm{dead}\rangle$.
  There's no *a priory* semantics for what's inside the ket.

Quantum mechanics: Pure state of Qubits

A Qubit is a quantum mechanical system whose state space has dimension 2, surprise surprise.

What the state space exactly is, is determined by the physical realization of the qubit. We don't want to bother.

Special orthonormal bases of 1-qubit systems:

- "Z-basis", "computational basis":
  $|0\rangle, |1\rangle$. What exactly these are depends on the physical realization — we don't want to bother.
- "X-Basis": $|+\rangle := \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, $|-\rangle := \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$
- "Y-Basis": $|\circlearrowleft\rangle := \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$, $|\circlearrowright\rangle := \frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle$

In this course, we only need finite dimensional Hilbert spaces

$$\mathbb{C}^N$$

Quantum mechanics: Pure states and superposition

Remember.
If the vectors $\psi_1, \dots, \psi_k$ *are* *<u>orthonormal</u>* *and* $\alpha_1, \dots, \alpha_k \in \mathbb{C}$*, then*

$$\left\|\sum_{j=1}^k \alpha_j \psi_j\right\|^2 = \sum_{j=1}^k |\alpha_j|^2$$

"Superposition": $\alpha|\Phi\rangle + \beta|\Psi\rangle$, $\alpha, \beta \in \mathbb{C}$

If a quantum system can be in states $|\Phi\rangle, |\Psi\rangle$, then it can be in any state which is a normalized superposition of the two.

Cannot be 0

"Make norm=1"

WTF With The Weird Notation?!??

- $\mathscr{A}, \mathscr{B}, \mathscr{C}, \mathscr{H}$ — Hilbert spaces
- ϕ, ψ, Φ, Ψ — vectors in H.S.
- $|\phi\rangle, |\psi\rangle, |\Phi\rangle, |\Psi\rangle$ — lin. mappings $\mathbb{C} \to \mathrm{H.S.}$
- $|\mathbf{x}\rangle, |\mathtt{cat}\rangle, |0\rangle, |+\rangle$ — also lin. $\mathbb{C} \to \mathrm{H.S.}$

  (operator $|\_\rangle$ is overloaded)
- $\langle \ldots|$ lin. mapping $\mathrm{H.S.} \to \mathbb{C}$
- $\langle\phi|, \langle\psi|, \langle\Phi|, \langle\Psi|$ — adjoints of $|\ldots\rangle$

- $\mathbb{C}^N$
- N-tuples
- N-by-1 matrices
- ...
- 1-by-N matrix
- Conjugate-transpose

$\psi = |\psi\rangle$ whenever we want it to be!

Combining systems

Postulate 2: Combined system.
If $\mathscr{A}$ is the state space of quantum system "Alice" and $\mathscr{B}$ is the state space of quantum system "Bob", then $\mathscr{A} \otimes \mathscr{B}$ is the state space of the combined system.

Remember.

1. In math notation: $(a' \otimes b' \mid a \otimes b) := (a'|a)\,(b'|b)$
2. If $|a_k\rangle$, $k = 1, \ldots, m$ is ONB of $\mathscr{A}$, and $|b_\ell\rangle$, $\ell = 1, \ldots, n$ is ONB of $\mathscr{B}$, then $|a_k\rangle \otimes |b_\ell\rangle$, $k = 1, \ldots, m$, $\ell = 1, \ldots, n$ is ONB of $\mathscr{A} \otimes \mathscr{B}$

Combining systems: n Qubits

The *computational basis* for a system of n qubits consists of these vectors:

$$|x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle$$

where $(x_1, \ldots, x_n) \in \{0,1\}^n$.

Abbreviations:

$$|x_1\rangle|x_2\rangle \ldots |x_n\rangle$$
$$|x_1, x_2, \ldots, x_n\rangle$$
$$|x_1 x_2 \ldots x_n\rangle$$

Careful! The convention that all of these are equal does not apply syntactically!

I.e., it depends on what is meant by $|1,1,0\rangle$.

Tensor expressions can look totally different, and still be equal:

$$|00\rangle + |11\rangle = |++\rangle + |--\rangle$$

Combining systems: *Warning!*

$$|x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle$$

$$|x_1\rangle|x_2\rangle \ldots |x_n\rangle$$

In $|\psi_1\rangle|\psi_2\rangle \cdots |\psi_{n-1}\rangle|\psi_n\rangle$

the implicit "·"'s between the factors is

"·" := "$\otimes$" — *NOT* "$\circ$" (concat of operators)

Same order!

$$\Big(|\psi_1\rangle|\psi_2\rangle \cdots |\psi_{n-1}\rangle|\psi_n\rangle\Big)^\dagger = \langle\psi_1|\langle\psi_2| \cdots \langle\psi_{n-1}|\langle\psi_n|$$

Now you know how to describe the state of a quantum computer.

Changing the state

Postulate 3: Time evolution.
Time-evolution in a closed quantum system is linear: Consider a quantum system at times $t_0 \leq t_1$*. There is a linear operator* U *such that: If QS at time* t_0 *is in state* $|\Psi_0\rangle$*, then at time* t_1 it's in state:

$$|\Psi_1\rangle := U|\Psi_0\rangle$$

- Remember: A linear operator $U : \mathscr{H} \to \mathscr{H}$ satisfying
$$\|U\psi\| = \|\psi\| \text{ for all } \psi$$
is called ***unitary***.
- The U in the postulate is unitary, because it maps states to states.

Changing the state: "Closed" vs "Isolated"

- Closed quantum system:
  - States are Hilbert space vectors of norm 1.
- *Isolated* quantum system:
  - The time evolution operator depends only on $t_1 - t_0$, i.e., it never "essentially" changes.
- Quantum systems used for quantum information processing are, ideally, closed, but they can be "controlled", i.e., the state-change operator can be modified — so they are not isolated.

What's going on?

Postulate 4: Projective Measurement.
Let $\mathscr{H}$ be the state space of a quantum system.

Let P_r, $r \in R$, be (orthogonal) projectors with sum $\mathbf{1}$ ("Identity operator").
One can measure P_* of the system.

Assuming the system is in state Ψ, this is what happens (in theory):

1. *The measurement returns an $r_0 \in R$*
2. *The state of the quantum system changes to $\frac{1}{\|P_{r_0}\Psi\|} P_{r_0}\Psi$*
3. *The selection of r_0 happens randomly, where*

$$\Pr(r_0 = r) = \|P_r \Psi\|^2$$

What's going on???

Remarks.

1. The only way to learn something about the state of a quantum system is through measurement — there's no other way!

2. Postulates 3 and 4 seem to be contradictory but they are not: Postulate 3 is for a closed quantum system only, i.e., one that doesn't leak information. In Postulate 4, obviously, we're getting information out.

3. Result of measurement is a random variable with range "set of indices of the projectors". The probability distribution is determined by the state...

(And indeed, quantum mechanics is illegal in 12 US states.)

Math remarks: Recall...

1. A linear operator P is a called (orthogonal) projector, if it is self-adjoint $P^\dagger = P$ and idempotent $P^2 = P$.

2. A linear operator P is a projector IFF the Hilbert space can be split as an orthogonal sum $\mathrm{Img}P \perp \mathrm{Ker}P$ and $P\psi = \psi$ for all $\psi \in \mathrm{Img}P$.

3. A normal(!) operator P is a projector IFF it has no eigenvalues other than $0, 1$.

4. If P is a projector, then $P\psi$ is the unique best approximation of ψ by a vector in $\mathrm{Img}P$.

5. $\sum_j P_j = \mathbf{1}$ IFF $\mathrm{Img}P_j$, (j), pairwise orthogonal and sum up to $\mathscr{H}$.

Quiz? (Only for math geeks!)

Give an operator with eigenvalues $0, 1$ that is not a projector!

Review of the math of rank-1 projectors.

1. For $\Phi \in \mathscr{H}$, the "bra" $|\Phi\rangle$ is a linear mapping $\mathbb{C} \to \mathscr{H}$: $|\Phi\rangle(\alpha) = \alpha\Phi$.
2. For $\Psi \in \mathscr{H}$, the "ket" $\langle\Psi|$ is a linear form: $\langle\Psi|(\psi) = (\Psi|\psi) = \langle\Psi|\psi\rangle$
3. For $\Phi, \Psi \in \mathscr{H}$, the "ket-bra" $|\Phi\rangle\langle\Psi|$ is a linear mapping $\mathscr{H} \to \mathscr{H}$:
   $|\Phi\rangle\langle\Psi|\,(\psi) = \Phi \cdot (\Psi|\psi) = |\Phi\rangle\langle\Psi|\psi\rangle$.
4. $|\Psi\rangle^\dagger = \langle\Psi|$, $\langle\Psi|^\dagger = |\Psi\rangle$, $(|\Phi\rangle\langle\Psi|)^\dagger = |\Psi\rangle\langle\Phi|$

5. $|\Psi\rangle$ is a state iff $|\Psi\rangle\langle\Psi|$ is a non-zero projector.

6. The range of $|\Psi\rangle\langle\Phi|$ is $\mathbb{C}\Psi$ (unless $\Psi = 0$).

Measurement in the computational basis:

take the family of projectors $|x\rangle\langle x|$, $x \in \{0,1\}^n$.

Measurement of a part of a combined system

Suppose you have a combined system $\mathscr{A} \otimes \mathscr{B}$, and you want to know something about the $\mathscr{A}$-part. You have your projectors on $\mathscr{A}$ ready, P_r, $r \in R$. But to measure the combined system, you need projectors on $\mathscr{A} \otimes \mathscr{B}$.

Identity operator

Luckily, the family of linear operators

$$P_r \otimes \mathbf{1},\ r \in R,$$

satisfies the condition in Postulate 4:
they are projectors summing to $\mathbf{1}_{\mathscr{A} \otimes \mathscr{B}} = \mathbf{1}_{\mathscr{A}} \otimes \mathbf{1}_{\mathscr{B}}$.

"Global phase"

Quiz.

Let $|\Psi\rangle$ be a state, and $\zeta \in \mathbb{C}$ with $|\zeta| = 1$.

Prove that, whatever sequence of unitary operations and measurements you apply, the results will be the same in these two situations:

1. You start with the system in state $|\Psi\rangle$
2. You start with the system in state $\zeta|\Psi\rangle$

States which differ only by a scalar multiple are indistinguishable. Now you can start philosophical discussions about whether they should be considered "equal". (Answer: They should not.)

Universal Quantum Computer

Universal quantum information processing

In a quantum computer, you have a number n of qubits, and you can:

1. Reset ("*prepare*") the state of a qubit to $|0\rangle$
2. Perform unitary operations from a restricted set of "gates" on 1 and 2 qubits (sometimes more)
3. Perform measurement (in the computational basis) of each qubit (projectors $|0\rangle\langle 0| \otimes \mathbf{1}, |1\rangle\langle 1| \otimes \mathbf{1}$)
4. Sending and receiving of qubits ("flying qubits").

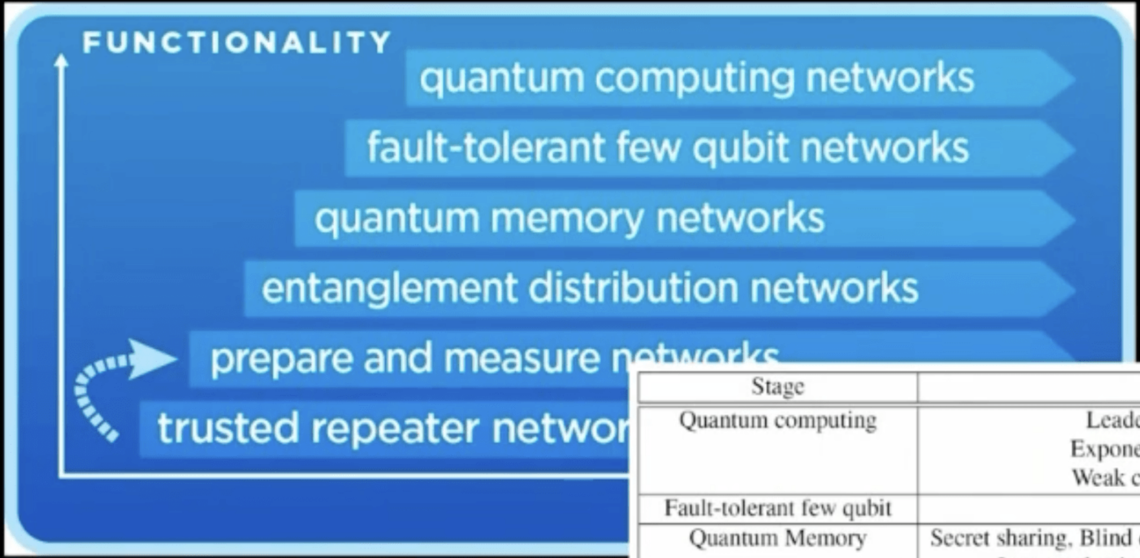
Subset of *DiVincenzo*'s criteria

Universality: The restricted gate set must be powerful enough so that any unitary on the whole 2^n-dimensional Hilbert space can be realized approximately, to arbitrary precision.

Quantum communication & computing

Functionality driven stages of a quantum internet

S. Wehner, D. Elkouss, R. Hanson - *Science - 362, 6412 (2018)*



Stage	Examples of known protocols
Quantum computing	Leader election, Fast byzantine agreement Exponential savings for communication tasks Weak coin flipping with arbitrarily small bias
Fault-tolerant few qubit	Clock synchronization
Quantum Memory	Secret sharing, Blind quantum computing (using remote quantum servers), Improved coin flipping, Anonymous quantum transmissions, Extending baseline of telescopes, Simple leader election and agreement protocols, Time limited clock synchronization
Entanglement Distribution	Device independence for QKD and other protocols in the prepare and measure stage
Prepare and Measure	Quantum key distribution (QKD), Two-party cryptography, Position verification, Imperfect coin flipping