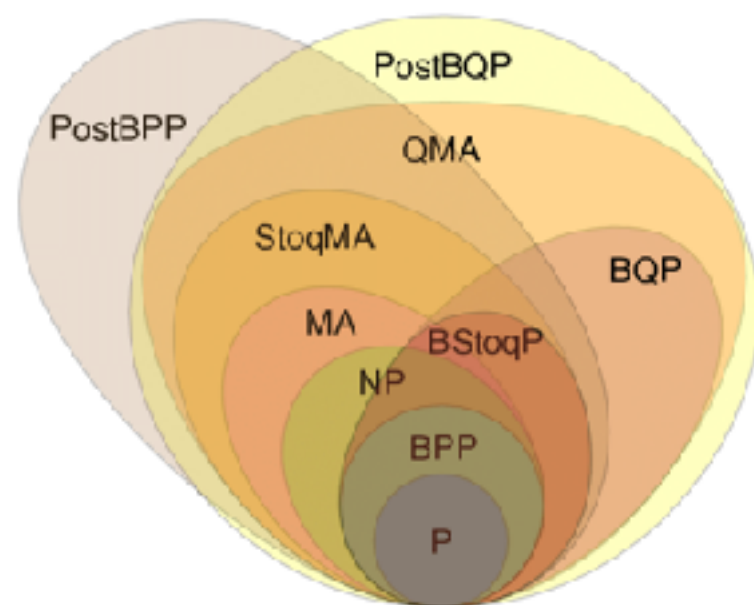


Quantum Complexity Theory

Lecture 1: a gentle introduction

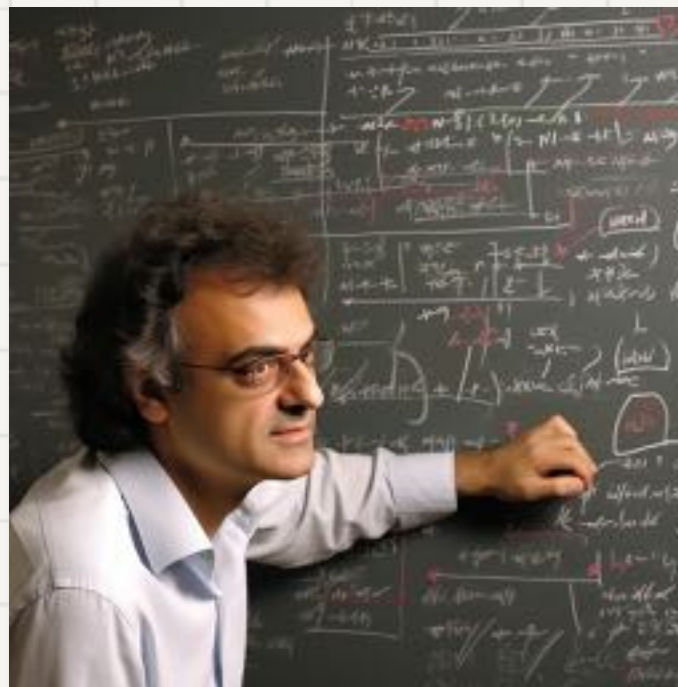
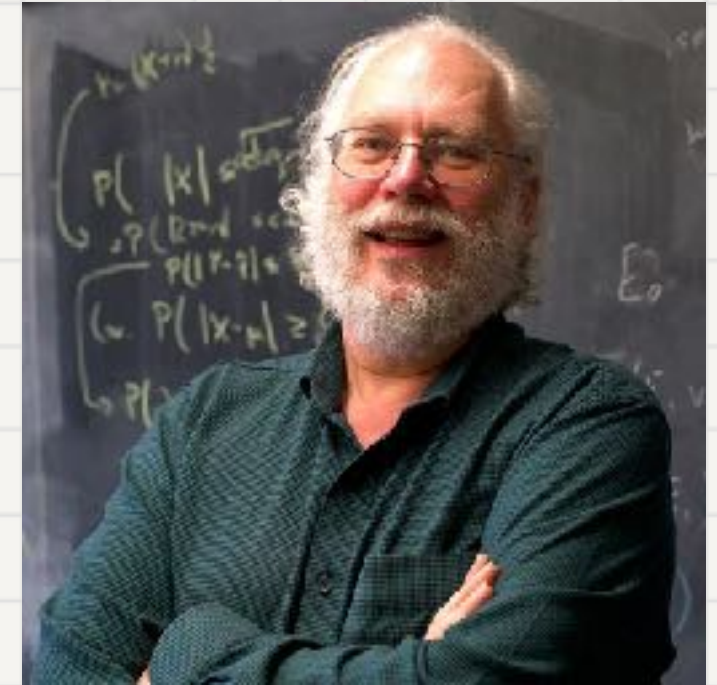
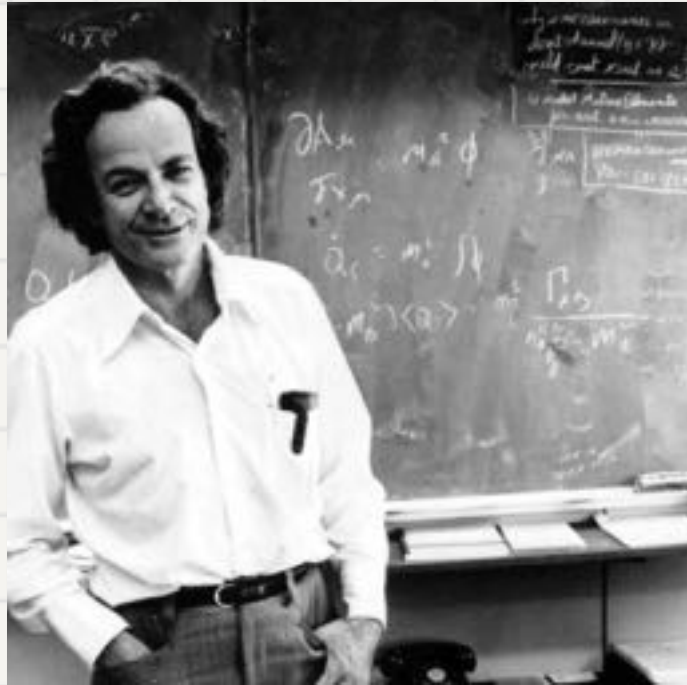


Tom Gur



UNIVERSITY OF
CAMBRIDGE

A story via a quiz: name the scientists



Quantum Complexity Theory

Goal: Understand the power and limitations of quantum computing

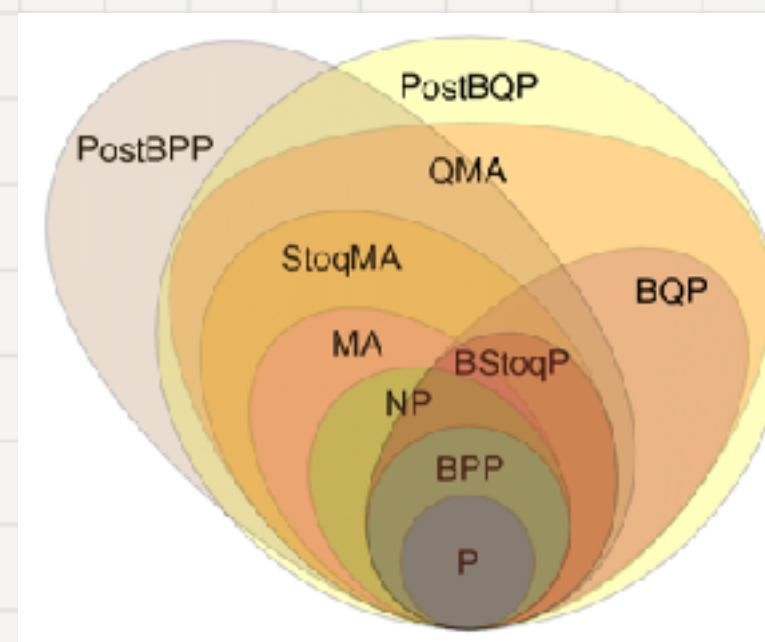
Why care?

Theory: Quantum computing as the “algebraic completion” of computing

Practice: Discover new quantum algorithms!

Interdisciplinary:

Deep connections to physics and mathematics



"if you teach a course on quantum mechanics, and the students don't have nightmares for weeks, tear their hair out, wander around with bloodshot eyes, etc., then you probably didn't get the point across."

Time travel

Parallel universes

Teleportation

Cloning

Faster-than-light communication

Determinism

Chaos

QUANTUM COMPUTING SINCE DEMOCRITUS



SCOTT AARONSON

Course structure

Part 1 Review/crash-course on quantum computing

Supporting material:

[Quantum computing lecture videos \(YouTube\)](#)

[Scott Aaronson's lecture notes](#)

Basics of quantum complexity theory

(Complementing Cambridge's Quantum Computing course)

Part 2 Advanced topics: Quantum PCP, learning algorithms,
zero-knowledge proofs, supremacy, lower bounds, and more...

Foundations of quantum complexity

Topic 1. Introduction and basics of Quantum Mechanics

Topic 2. Bell's inequality

Topic 3. BQP and QMA

Topic 4. Fourier sampling

Topic 5. Mixed states

Advanced Topics

Topic 6. Quantum PCP and NLTS

Topic 7. Quantum Interactive Proofs

Topic 8. $\text{MIP}^* = \text{RE}$

Topic 9. Quantum Zero-Knowledge Proofs

Topic 10. Quantum Supremacy: Yamakawa-Zhandry

Other topics. Quantum Cryptography, distributed computing, circuit synthesis

Exam on 30 November

Anonymous feedback

A chance to make a difference

in time for this term!

Anonymous Feedback

Quantum Complexity Theory

 Not shared

Please feel free to leave any comments, suggestions, and requests. If things are going well, a good word is always appreciated. If you have ideas on improving the course, please let me know (in a kind and respectful way). I hope you enjoy the course!

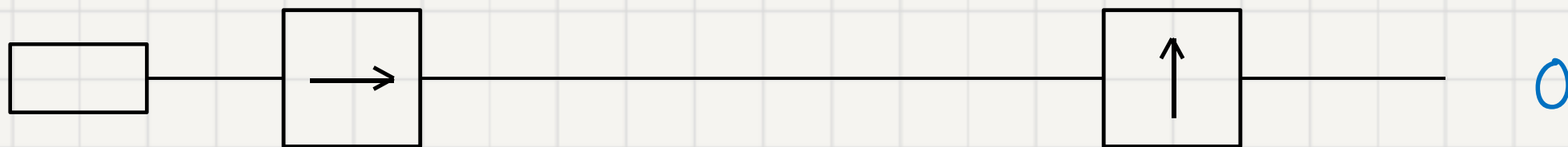
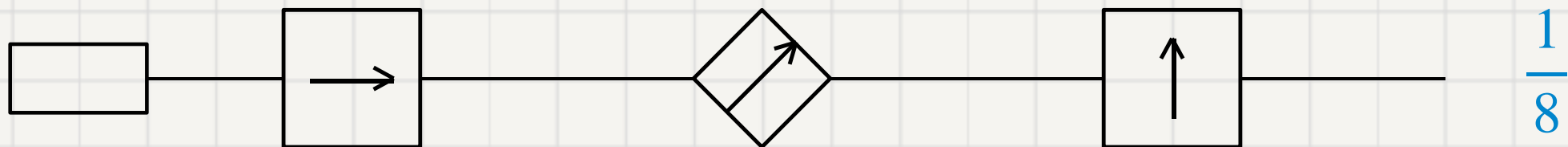
Your answer

<https://www.cl.cam.ac.uk/teaching/2627/L330/materials.html>

A crash course
on
Quantum Computing

Non-commutative probability theory

The 3 filters experiment



Classical: $\frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{8}$

Quantum: $H = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad D = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \quad V = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$

$$H \cdot V = 0 \neq HDV$$

The "postulates" of classical (stochastic) computation

Postulate 1 (Randomness)

Consider a machine with memory tape containing n bits

Let $s_1, \dots, s_{2^n} \geq 0$, $\sum_i s_i = 1$ be a distribution over n bit strings,

represented by $\begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_{2^n} \end{bmatrix} \in \mathbb{R}^n$

Postulate 2 (Measurement)

Observing/measuring gives i w.p. s_i . Then randomness collapses.

Postulate 3 (Stochastic computation)

S evolves stochastically $s \mapsto A \cdot s$, where $A = \{a_{ij}\}$ and

$$a_{ij} \geq 0, \forall j \sum_i a_{ij} = 1$$

maps distributions to distributions

Postulate 4 (Composite systems)

Systems S and T combined are represented by $S \otimes T$.

E.g., for $\begin{bmatrix} s_1 \\ s_2 \end{bmatrix}$ and $\begin{bmatrix} t_1 \\ t_2 \end{bmatrix}$, the tensor $\begin{bmatrix} s_1 \\ s_2 \end{bmatrix} \otimes \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} = \begin{bmatrix} s_1 t_1 \\ s_1 t_2 \\ s_2 t_1 \\ s_2 t_2 \end{bmatrix}$

From Stochastic to Quantum

Interlude: a paradox?

Quantum mechanics is a linear theory

Classical mechanics is non-linear

But QM is more general: how is that possible?

Dirac's bra-ket notation

Consider $\mathbb{C}^d$. Denote $|i\rangle = e_i \quad \forall i \in [d]$

$$|\psi\rangle = \sum_i \alpha_i |i\rangle$$

$$\langle\psi| = \left(|\psi\rangle\right)^* = \sum_i \alpha_i^* \langle i|$$

"bra": Hermitian-conjugate row vector

"ket"

column vector

$$\begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} \leftarrow i$$

Inner and outer products

Inner product: $\langle \theta | \psi \rangle = \sum_i \alpha_i \beta_i^*$

Outer product: $|\psi\rangle\langle\theta| = M, \quad M_{ij} = \alpha_i \beta_j^*$

$$M = \sum_{i,j} M_{ij} |i\rangle\langle j|$$

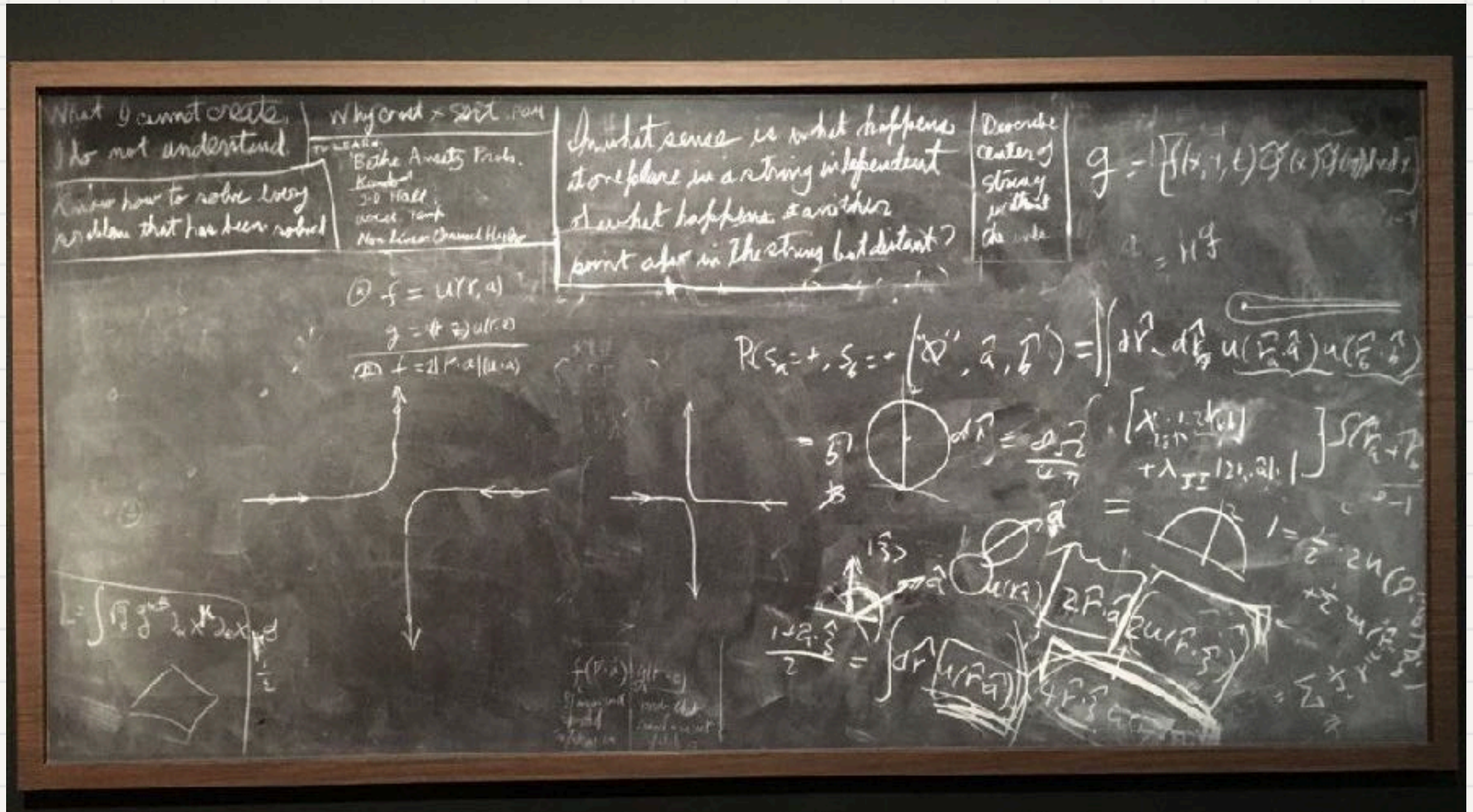
For $M = |\psi\rangle\langle\theta|$ and $v = |\phi\rangle$:

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

matrix x vector

vector x scalar

Quote of the day



What I cannot create, I do not understand — Richard Feynman

Postulate 1 (Superposition)

A quantum state is a vector $|\psi\rangle \in \mathbb{C}^d$ such that

$$|\psi\rangle = \begin{bmatrix} \alpha_0 \\ \vdots \\ \alpha_{d-1} \end{bmatrix} \qquad \left\| |\psi\rangle \right\|_2^2 = \langle \psi | \psi \rangle = \sum_{i=0}^{d-1} |\alpha_i|^2 = 1$$

Ex: Qubit $\begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix} \in \mathbb{C}^2$ s.t. $|\alpha_0|^2 + |\alpha_1|^2 = 1$

amplitudes (vs probabilities)

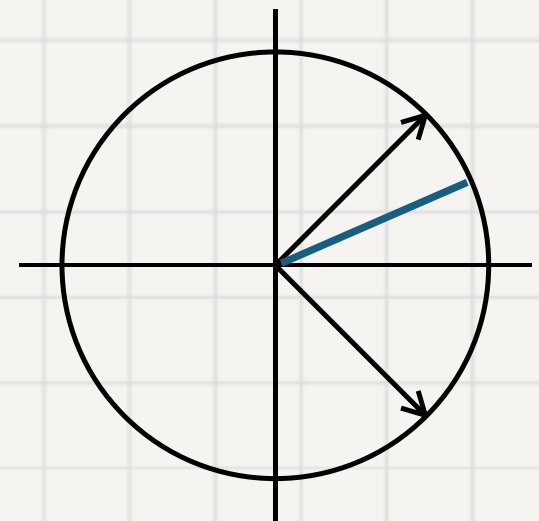
Two "novelties": ① complex numbers (negative?!)

② ℓ^2 -norm

Postulate 11 (Measurement)

Measuring a state $|\psi\rangle = \sum_i \alpha_i |i\rangle$ in an orthonormal basis $\{|b_0\rangle, \dots, |b_{d-1}\rangle\}$

collapses it to $|b_i\rangle$ with probability $|\langle b_i | \psi \rangle|^2$



Ex (Born's rule)

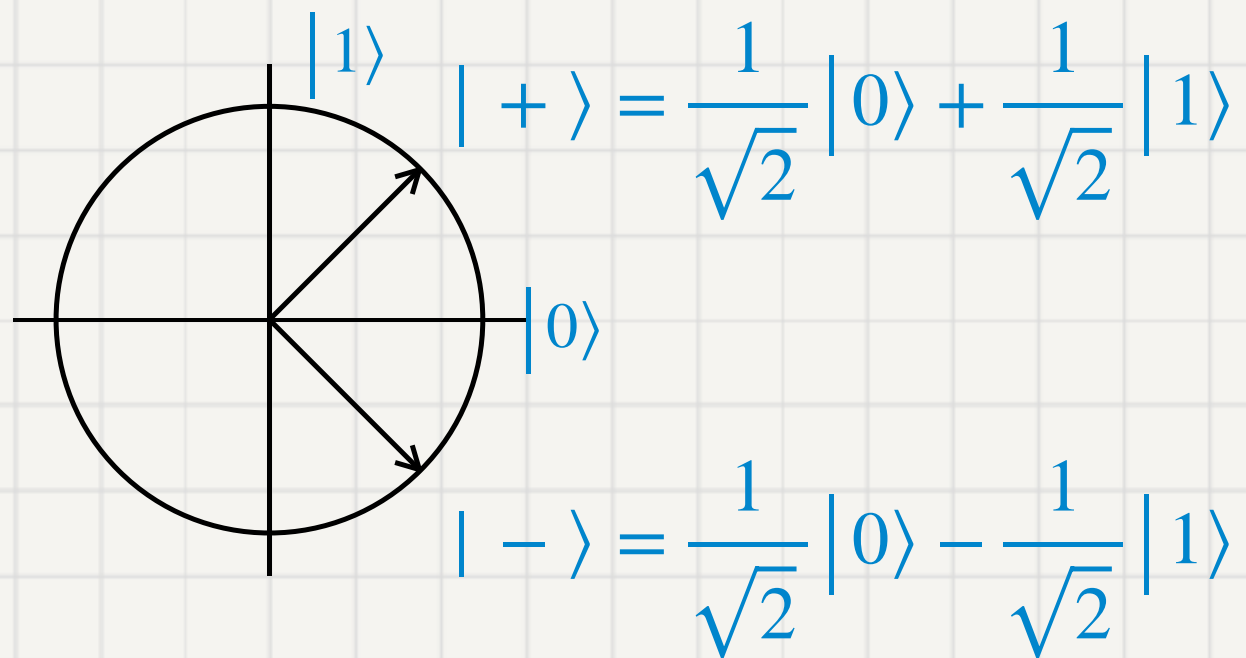
Measuring $(\alpha_0, \dots, \alpha_{d-1})^T$ in the computational

basis $\{|e_i\rangle\}$ collapses it to $|i\rangle$ w.p. $|\alpha_i|^2$

Most famous footnote!

Example: Qubit measurement

Qubit $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$



Postulate III (Unitary evolution)

Quantum states evolve via unitary transformations,

$$|\psi\rangle \rightarrow U|\psi\rangle, \text{ where } UU^\dagger = I \quad (\text{Hence } U^{-1} = U^\dagger)$$

- U maps unit vectors to unit vectors.

(quantum states)

- U preserves inner products

$$\langle \psi | U^\dagger U | \theta \rangle = \langle \psi | U^{-1} U | \theta \rangle = \langle \psi | \theta \rangle$$

Example: Single-qubit gates

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

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

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

Pauli matrices

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

Hadamard gate

Postulate IV (Composite systems)

The joint state of $|\psi\rangle$ and $|\theta\rangle$ is $|\psi\rangle \otimes |\theta\rangle$

$$\text{Ex } |0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \qquad |0\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \qquad \dots$$

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle, \quad |\theta\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle$$

$$|\psi\rangle \otimes |\theta\rangle = \begin{bmatrix} \alpha_0 \beta_0 \\ \alpha_0 \beta_1 \\ \alpha_1 \beta_0 \\ \alpha_1 \beta_1 \end{bmatrix} = \alpha_0 \beta_0 |00\rangle + \alpha_0 \beta_1 |01\rangle + \dots$$

Entanglement

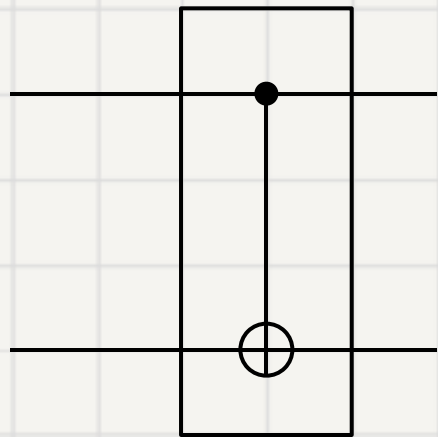
States that are not tensor products are entangled.

Example: an EPR pair

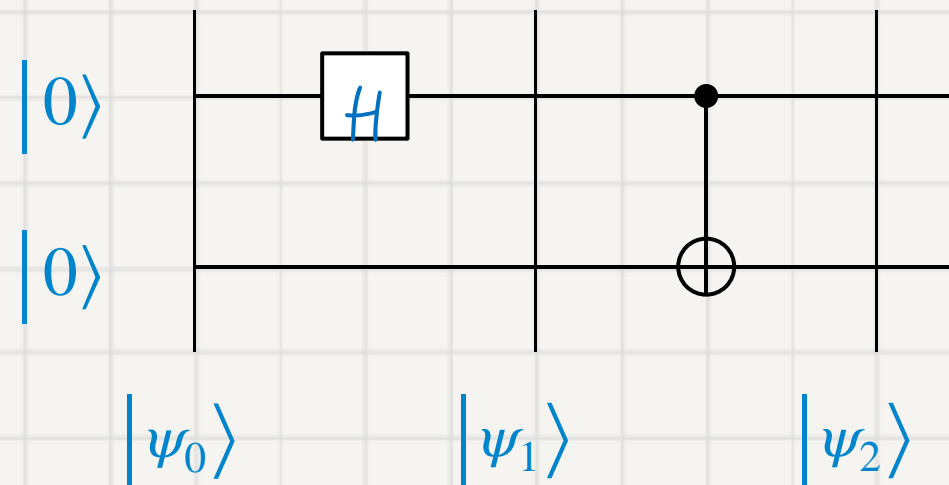
$$|\text{EPR}\rangle = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$$

Preparing an EPR pair

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



$$\begin{array}{l} |00\rangle \rightarrow |00\rangle \\ |01\rangle \rightarrow |01\rangle \\ |10\rangle \rightarrow |11\rangle \\ |11\rangle \rightarrow |10\rangle \end{array}$$



$$|\psi_0\rangle = |00\rangle$$

$$\begin{aligned} |\psi_1\rangle &= |+\rangle \otimes |0\rangle \\ &= \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |10\rangle \end{aligned}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle = |\text{EPR}\rangle$$