JOHN PRESKIL.

PHYSICS + COMPUTER SCIENCE

Quantum computation

(density op, quantum op, entanglement, circuit, quantum algorithm)

Level II : Quantum Error correction (soon.)

(Planck) (Turing) (Shanon)

Quantum theory + computer science + info. theory

= Quantum Info science

QUANTUM INFORMATION SCIENCE

i) Quantum sensing
ii) Quantum cryptography
iii) Quantum Networking
iv) Quantum Simulation
v) Quantum computing
vi) Quantum information concepts

Two fundamental ideas

(1) Quantum Complexity
(why we think Quantum Computing is powerful)

(2) Quantum Error correction
(why we think quantum computing is scalable?)

# Quantum Entanglement

## classical book and Quantum Book

The information does not reside in the pages. It is in the coorelations between the pages. You can't access the information if you read the book one page at a time.

A complete description of a typical quantum state of just 300 qubits require more bits than the number of atoms in the visible universe

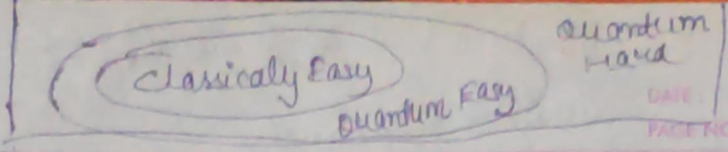
Why we think Quantum Computing is powerful?

(1) Problems believed to be hard classicaly, which are easy for quantum computers. Eg. factoring

(2) Complexity theory arguements indicating that quantum computers are hard to simulate classicaly.

(3) We don't know how to simulate a quantum computer efficiently using a digital ("classical") computer. The cost of the best known simulation algorithm rises exponentially with the number of qubits

But... the power of quantum computing is limited. We don't believe that quantum computers can efficiently solve worst-case instances of NP-hard optimization problem.




## The Theory of Everything

The theory of everything is not even remotely a theory of every thing.

We know this equation is correct. However it cannot be solved accurately when the number of particles exceed about 10. No computer existing or that will ever exist can break the barrier, because it will be a catastrophe of dimension.

RB Laughlin and D. Pines

Why quantum computing is hard?

→ We want qubits to interact strongly with one another.

→ We don't want qubits to interact with the environment

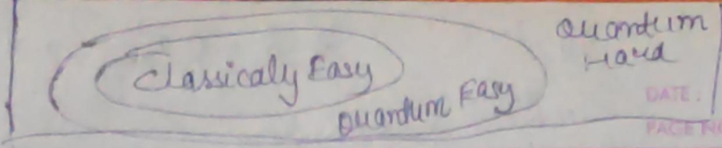
→ Except when we control or measure them.

Decoherence

$$\frac{1}{\sqrt{2}}\Big(\text{wake} + \text{sleep}\Big)$$

Environment

Decoherence explains why quantum phenomena, though observable in the microscopic system studied in physics lab, are not manifested in the macroscopic physical systems that are encounter in our ordinary experience






## The Theory of Everything

The theory of everything is not even remotely a theory of every thing.

We know this equation is correct. However it cannot be solved accurately when the number of particles exceed about 10. No computer existing or that will ever exist can break the barrier, because it will be a catastrophe of dimension.

RB Laughlin and D. Pines

## Why quantum computing is hard?

- → We want qubits to interact strongly with one another.
- → We don't want qubits to interact with the environment
- → Except when we control or measure them.

## Decoherence

$$\frac{1}{\sqrt{2}}\left(\text{wake} + \text{sleep}\right)$$

Environment

Decoherence explains why quantum phenomena, though observable in the microscopic system studied in physics lab, are not manifested in the macroscopic physical systems that are encounter in our ordinary experience

Quantum Decoherence Environment
computer → ERROR.

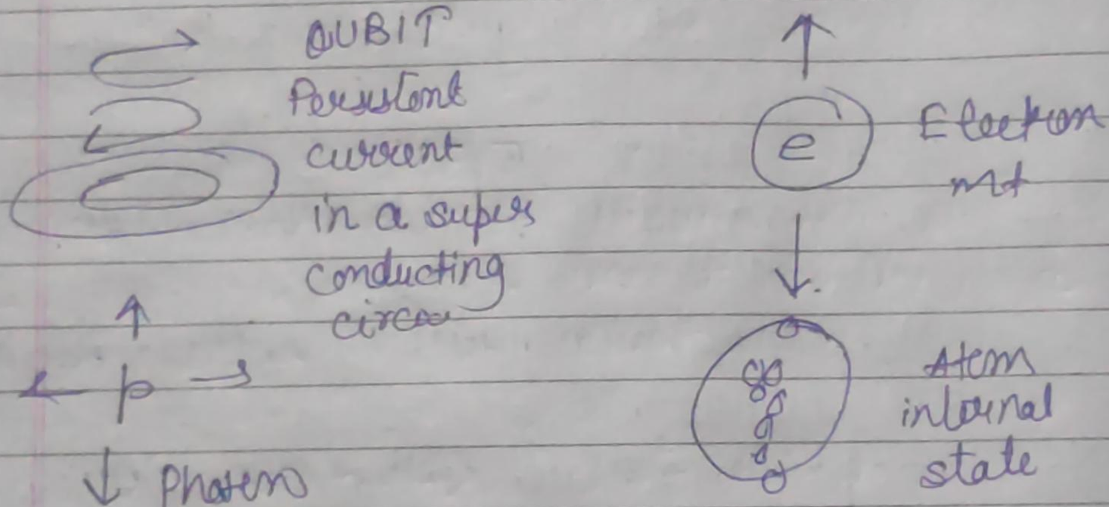
DATE :
PAGE NO. :

To resist decoherence, we must prevent the environment from "learning" about the state of quantum computer during the computation

Quantum Error Correction

The protected "logical" quantum information is encoded in a highly entangled state of many qubits.

The environment can't access this information if it interacts locally with the protected system.




Intrinsic resistance to decoherence

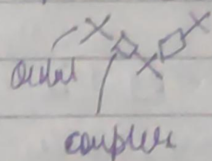
classical systems cannot simulate quantum systems efficiently

About Sycamore

Quantum David vs Classical goliath

A fully programmable circuit-based qc (n=53) working qubits in 2-d array with coupling of nearest neighbors

circuit with 20 layers of 2-qubit gates executed million times




HYBRID QUANTUM / CLASSICAL

measure cost func

Quantum Processor → classical optimizer

←

adjust quantum circuit

The era of quantum heuristics

Sometimes algorithms are effective in practice even though theorists are not able to validate their performance in advance Eg: Deep Learning

Possible quantum examples:

Quantum Annealers, approximate opt.
qml.

dialog b/w quantum algo experts and application users.

QEC carries a high overhead cost in number of qubits and gates

20 million physical qubits to break RSA 2048, for gate error rate $10^{-3}$



Quantum Error Correction ⇄ HYBRID

Quantum Info v/s classical info.

1) Randomness : clicks in Geiger counter are intrinsically random, not pseudo random.

2) Uncertainity: operators 'A' and 'B' do not commute means that measuring A influences B

3) Entanglement: The whole is more definite than the parts.

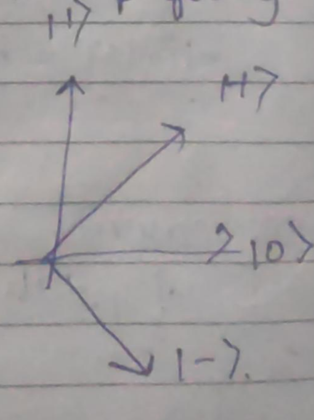
QUBIT

A vector (actually a 'ray' because the normalization is 1, and overall phase does not matter) in a two dimensional complex Hilbert space.

$$|\psi\rangle = a|0\rangle + b|1\rangle \qquad |a|^2 + |b|^2 = 1$$
$$a, b \in \mathbb{C} \qquad |\psi\rangle \sim e^{i\alpha}|\psi\rangle$$

Two orthogonal states $|0\rangle$ and $|1\rangle$ are perfectly distinguishable

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$$



Prove it:

Best chance of winning: $\cos^2\left(\frac{\pi}{8}\right) = 0.853$

if Alice send either $|1\rangle$ or $|+\rangle$

Quantum Key Distribution

Non-orthogonal states cannot be perfectly distinguishable

Information vs. disturbance

Suppose Alice prepares either $|\varphi\rangle$ or $|\psi\rangle$. To distinguish them, eve performs a unitary transformation that rotate's her probe, while leaving Alice's state intact.

$$U: \quad |\varphi\rangle_A \otimes |0\rangle_E \longrightarrow |\varphi\rangle_A \otimes |e\rangle_E$$
$$|\psi\rangle_A \otimes |0\rangle_E \longrightarrow |\psi\rangle_A \otimes |f\rangle_E$$

U: unitary, hence preserves inner product

$$\langle\psi|\varphi\rangle \cdot \langle f|e\rangle = \langle\psi|\varphi\rangle$$

and if $|\psi\rangle$ and $|\varphi\rangle$ are non-orthoganal

then $\langle f|e\rangle = 1$

states are same

Eve's measurement of the probe cannot reveal any info. about the state.

On the other hand if $|\varphi\rangle$ and $|\psi\rangle$ are orthogonal, the probe state can also be orthogonal and Eve can copy that info.

"We can't distinguish non-orthogonal states without disturbing them".

# Tensor product.

System divided into two

A

$\{ |i\rangle_A,\ i = 1, 2, \ldots d_A \}$

B

$\{ |a\rangle_B,\ a = 1, 2, \ldots d_B \}$

Basis states of the composite system are distinguishable if they can be distinguished on either Alice's or Bob's.

$$(\langle j| \otimes \langle b|)(|i\rangle \otimes |a\rangle) = \delta_{ij}\,\delta_{ab}$$

$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ are all distinguishable

## Many Qubits

$A_1$ $A_2$ $A_3$ $A_4$ $A_5$ … $A_n$

$$\mathbb{C}^{2^n} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$$

spanned by

$$|x\rangle = |x_{n-1}\rangle \otimes |x_{n-2}\rangle \otimes \cdots \otimes |x_1\rangle \otimes |x_0\rangle$$

$$x \in \{0,1\}^n$$

where $\langle x|y\rangle = \delta_{x,y}$

For 300 qubits, vector in a space with dimension $2^{300} \sim 10^{90}$ more than the number of atoms in visible universe.

which decomposition into subsystem?

→ Typically dictated by spatial locality.

DATE:
PAGE NO.

A product state

$$|\Psi\rangle = |\psi_1\rangle_{A_1} \otimes |\psi_2\rangle_{A_2} \otimes \cdots \otimes |\psi_n\rangle_{A_n}$$

has succinct description; only $2n$ real params.

## Entanglement

If a pure state is not a product state, it is entangled.

$$\boxed{A_k} \rightleftarrows \boxed{A_{k+1}}$$

## Quantum computer: the circuit model

(1) Hilbert space of '$n$' qubits

$$\mathcal{H} = \left(\mathbb{C}^{2^n}\right)$$

spanned by

$$|x\rangle = |x_{n-1}\rangle \otimes |x_{n-2}\rangle \otimes \cdots \otimes |x_1\rangle \otimes |x_0\rangle$$

$$x \in \{0,1\}^n$$

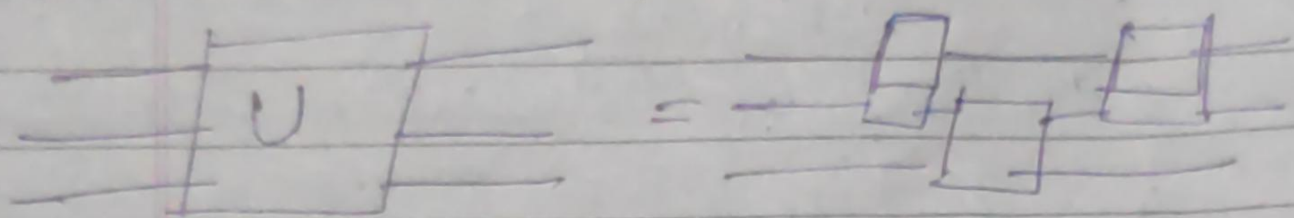
The Hilbert space is equipped with a natural tensor product decomposition into subsystems

$$\mathbb{C}^{2^n} = \underbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n \text{ times}}$$

Physically, this decomposition arises from spatial locality.

(2) Initial state $|000\ldots00\rangle = |0\rangle^{\otimes n}$

(3) A finite set of fundamental quantum gates
$\{U_1, U_2, \ldots U_{n_q}\}$
Each gate is a unitary transformation acting on a bounded number of qubits.



(4) Classical control
The construction of a quantum circuit is directed by a classical computer i.e Turing Mach

(5) Readout
At the end, we read the result by measuring $\sigma_z$ i.e projecting onto $|0\rangle, |1\rangle$