I. lutroduction

What is Quantum Information Theory?

- > The study of reformation processing using Hu laws of quantum mechanics

Quartum mechanics / quartum Kicory: The most juncal francwork to describe mother at the fundamental (microscopic) level.

Quantum Kicovis exits for almost all classical physical Kiemes: mechanics (i.e. motor of particles subject to forces), electrody using, ... - except granty.

Here, q. unecharais (or q. Knory, or q. phypes) always refers to the general framework.

Whey sterild we shall information processing in the frame work of quantum Keerry?

Even purters: Whey deald we study reformation processing in the context of plugpes?

Information is a priori a concept un clated to its physical realitation (modern computer, punchcard, releys, paper, ...) - destical ufornaha Herry (Shaunon Keery) secur talks about playsies.

dandans (1961): Erang nformalia creaks heat:



∆S₈₄₅ = -k lu 2 = AQ eu = -TAS₈₄₅ = kT lu 2

→ Erasny 1 bit releases sQ = kT lu 2 heat -rude pendent of realizable.

Jaudans: "Information is physical" (i.e. we need to take at least the pundamental pluys portuciples noto account when thinking about nfo. processing in real systems.) On the other hand: "Roon's law" -> # transistors/chip doutes every 18 marthes - A bransistor site eventually approaches atomic hite! - und take quarken effects into accort: eiter fight theen or rese them. - Quantien beformation Recory -> heformation processing taking ruto account

the fundamental porneigles of q. Kecory - redependent of specific plequical

realitation.

3

Basic poruciples, I deas, and applications of QI

Classical nformation: bit 6=0,1 Quantum rufo: quantum 6st (quáit) with two basis rectors $\vec{e}_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \vec{e}_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. General qu'est configuration ("stak") is a superposition $\binom{\alpha}{\beta} \in \mathbb{C}^2$, $|\alpha|^2 + |\beta|^2 = 1$

Kas pruilantes to prot. destributions over classical tits, $\begin{pmatrix} T^{\circ} \\ P_{i} \end{pmatrix}$ with $P_{\circ}, P_{i} \ge 0$, $P_{\circ} + P_{i} = 1$, but also hey differences.

"Requirement": Can diech (test, marine) the value of a classical bit (e.g. con ma sox) prepared m a state (Po).

-> updake shere (1)

(2nd masurement gives same repult (no new ruto), 5 - V meagnement "collapses" state.

Restrance of queenhow 5.7: and the of the content of the case of the case of the content of the case of the content of the rue possible uncamenant kut offier reacquicterents east, e.g.: Careb: prob. lx+\$12 (x) } Kernlt "+" Diferent possibilities can cancel prote la-B12) Result 4_4 "Dastmichte niterferene What is the state after uncare cueant? - Same portreiple: 2x same neas. - J same result! <u>Carea</u>: Brate after mæs: (1) or (2) Care 6: Stete after meas: $\begin{pmatrix} \frac{1}{12} \\ \frac{1}{12} \end{pmatrix}$ or $\begin{pmatrix} \frac{1}{12} \\ -\frac{1}{12} \end{pmatrix}$,

pro6: 2 2	
-----------	--

Reasoning me "property" can affect other : Proposhies ar unde rideprendent. There is no 1-to-1 correspondence Schween Ree unuders (x) and properties we can measure.

 $\frac{1}{2}$ $\frac{1}{2}$

Consequeries: 0 "No-clocerty-Keeoren" Quantum Information cannot be capital, i.e., a device $\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \rightarrow \boxed{\begin{pmatrix} \alpha \\ \beta \end{pmatrix}} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ does not exist!

(Othermik,	۲ ۰۲	could	dekruire	$(\frac{1}{\lambda})$	exactily,	and
per ca fre a	d.J.	quant	sities at h	ne farm	2 true.)	

(Nok: The same hold for class. prob. distributions.)

7

o Quantum Crypto frapley Dong meas. disherts grean hem dak ; \mathcal{C} send q, Hate earesdropper "Eve" A "Rob " "Alice"

Reasurement disherts state -> Eve cannot astain mformation about state stend without ABB which -> can be used to establish secret keys.

o Eutanplement, klepstaka, Rell megualities

A ABB share jort state: distribution over $00, 01, 10, 11: \begin{pmatrix} x \\ \beta \\ \gamma \end{pmatrix} \stackrel{00}{}_{10}$

Can choose state such that outcomes are perfectly correlated for all measurements.

Their can also heppen a classical theory; A "hidden varable encodel" has an independent pre-détercurred outcome for every test (like a corr). Bret: A local beidden varable (LHV) model

Vars(A) (Comparison (Compariso where the boxes caused communicate (-> relating!) satisfies special maqualities (" Bell megualities ") which are notated by quantum dates ? -> " Eutanglement"

-> Q. T. states can display un - clattical correlations. But: No faster-Kian- light comanucication possible!!

Theis also highlights a facedomental defenue Schreen probability know and quantum theory: In prob. K., values are real indep. of incohercinent, and the stek (P) merely similies a lock of leaveledge. Quantum Keery does not allow for hich an nterpritation.

Releportation: A wants to get 9, State to 8, colour 9 rishery to love state. But No-clowing Ken -> A Caund make copies. -> Peleportaho: stak jont state State "appears" at B! - Does this allow for Jask - than - hight concern,? -> No! State on B's side is "scrawled" and requires A's weas. outcome (sent as classical refo at speed of light) to be

decoded!

Note: Ree <u>state</u> of the system is teleported, inst the system itself. (Asher Feres: "discuboolied researcher")

10 o Quantum Camputry: Typical hard comprahad proteen: "NP problems" : Solution may be leard to prod, but cary to check. E.g. frak colony: Can ve color pirce prophe with e.g. 3 colors sfort same color on adjacent vertices? Ceiven solution: easy to check! Quaetrece competer: Work isthe quaetrum tord?! - Supopondia of all possibiles? - D Right beake to check all solubous at the same place - D But: How can we sight out the good solutors? Non - mind profleen! (Note: For class, pool. distr. it also looks like we can test "all possibilities", but there, the's only

discortes randomly terry passibilities. 11 What is different on QT? -> Negable munders!) Shor '94: Quantum computers can Jactor unubers expression fally faster than any hearn classical algoritum.

Quentum Error Correction:

Noise can destroy quantum reformation! Any killed of influence for the outside!





0 -> 000 error, c.g. 001 correction \longrightarrow 1 -> 111 110 maj: vok Jup but 3 ¹/

-> Decreaks speche error rak!

0

Quantum lufo: scoral issues!

· clouing nu possible. • meas. destroys q. thete -> less to do majority vote? · errors can de catinuous - is it we possible to identify the error?

-> Quantum Error Correction! Use quantum superpositions to protect quantum Superposidas.