

Title: Introduction to Quantum Information

Date: Dec 09, 2008 10:00 AM

URL: <http://pirsa.org/08110056>

Abstract:

Introduction to quantum information

YRC, Dec 9th 2008



Quantum information theory

Quantum information theory

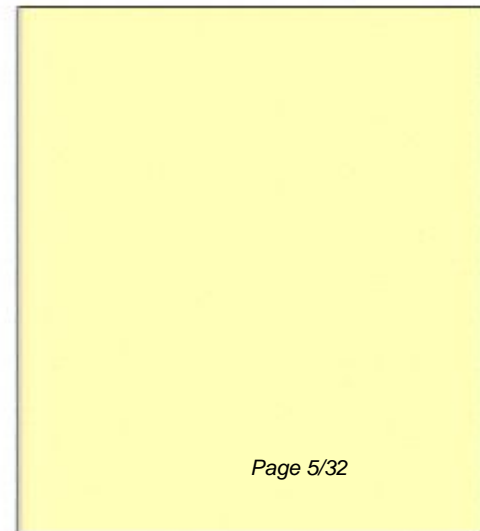
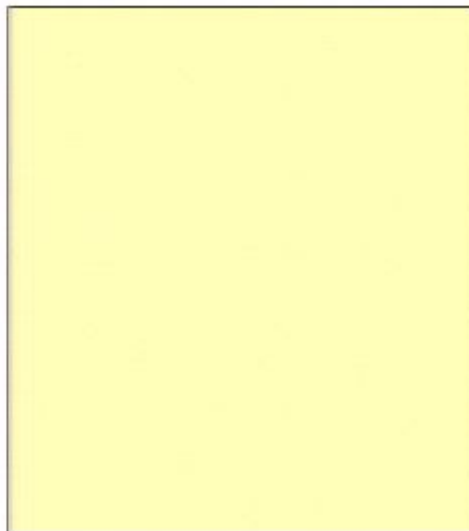
Quantum mechanics is really about the properties of physical information.

- Probabilities, expectations, etc...
- Operational language – measurements, transformations, outcomes.

Quantum information theory

Quantum mechanics is really about the properties of physical information.

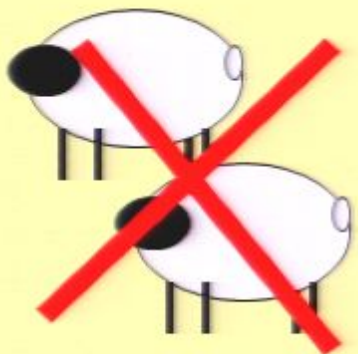
- Probabilities, expectations, etc...
- Operational language – measurements, transformations, outcomes.



Quantum information theory

Quantum mechanics is really about the properties of physical information.

- Probabilities, expectations, etc...
- Operational language – measurements, transformations, outcomes.



No cloning

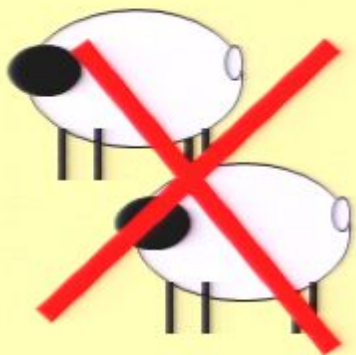


Teleportation

Quantum information theory

Quantum mechanics is really about the properties of physical information.

- Probabilities, expectations, etc...
- Operational language – measurements, transformations, outcomes.



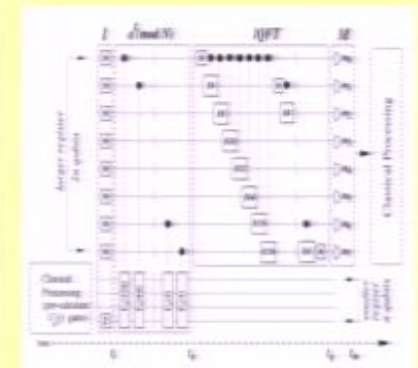
No cloning



Teleportation



Q Cryptography



Q Cryptanalysis

QUANTUM STATE 'N STUFF IN \mathbb{C}^2 (eg. Photon Polarization, Electron Spin, ...)

Pure Quantum States $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ ($= \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, $\alpha^* \alpha + \beta^* \beta = 1$)

$|\psi\rangle = e^{i\delta} (\cos\theta|0\rangle + e^{i\phi} \sin\theta|1\rangle)$

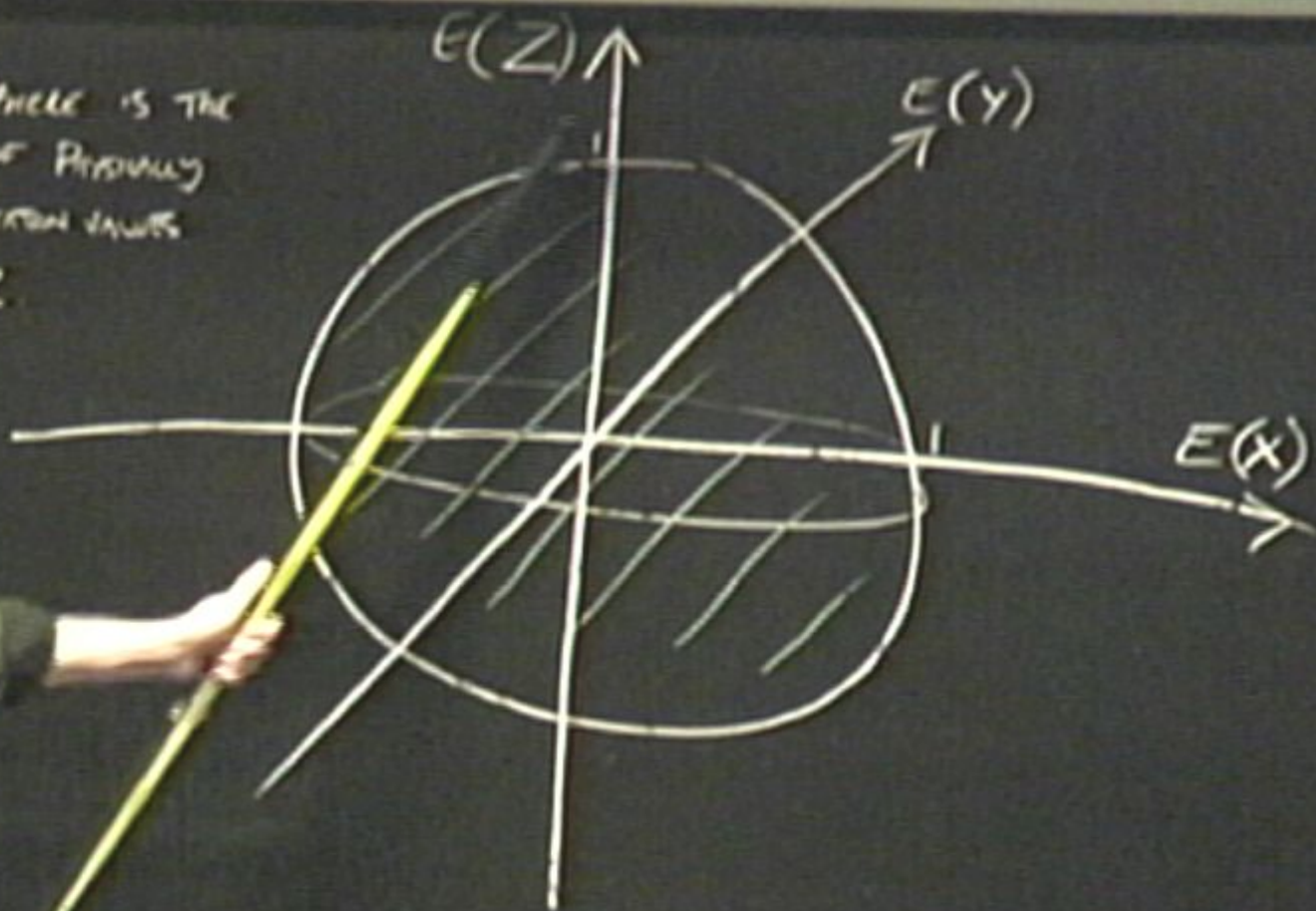


OBSERVABLES $A \in M_2 : A = A^\dagger$

Self-Adjoint (HERMITIAN) MATRICES

	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
EIGENVALUES & EIGENVALUES	$\frac{1}{\sqrt{2}}(0\rangle + 1\rangle) + 1$ $\frac{1}{\sqrt{2}}(0\rangle - 1\rangle) - 1$	$\frac{1}{\sqrt{2}}(0\rangle + i 1\rangle) + 1$ $\frac{1}{\sqrt{2}}(0\rangle - i 1\rangle) - 1$	$ 0\rangle + 1$ $ 1\rangle - 1$

THE BLACK SPHERE IS THE
CONVEX SET OF PHYSICALLY
ALLOWED EXPECTATION VALUES
FOR X, Y, Z .



MIXED QUANTUM STATES:

CONVEX SUMS OF PURE STATES

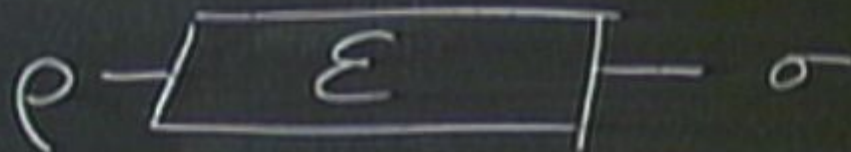
$$\rho = a|\psi\rangle\langle\psi| + b|\phi\rangle\langle\phi| + \dots$$

$$\rho \in M_2: \text{Tr}\rho = 1, \rho = \rho^\dagger, \rho \geq 0$$

Trace one, Hermitian, Positive Semidefinite

e.g. $\rho = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$. Maximally mixed state.

QUANTUM CHANNEL: DETERMINISTIC QUANTUM OPERATIONS



E is trace-preserving

GENERAL OPERATIONS: \mathcal{E} CP MAPS

GENERAL OPERATIONS : \mathcal{E} CP MAPS

$$\rho \xrightarrow{\mathcal{E}} \rho' \quad \sigma \quad \rho = \text{Tr}(\mathcal{E}(\rho))$$

\mathcal{E} must be trace non-increasing

linear

positive

completely positive! $(\forall \rho \in \mathcal{A}, I \otimes \rho \geq 0)$

Kraus form: $\mathcal{E}(\rho) = \sum_j E_j \rho E_j^\dagger, \left(\sum_j E_j^\dagger E_j \leq I \right)$

Nonorthogonality and uncertainty

Quantum states can be **nonorthogonal**.

For example, $|0\rangle$ is not orthogonal to $\alpha|0\rangle + \beta|1\rangle$.

Their inner product is α .

Linearity upper bounds the probability that these states would behave differently when something – anything at all – is done to them. With probability at least $\alpha^* \alpha$ they'll behave identically.

This is a huge difference from 'classical' physics, where points in phase space are arbitrarily distinguishable.

Uncertainty

Different observables won't commute – their eigenstates are nonorthogonal.

Measurement disturbance

Preparing an eigenstate of one observable overwrites information about other observables.

Nonorthogonality and uncertainty

Quantum states can be **nonorthogonal**.

For example, $|0\rangle$ is not orthogonal to $\alpha|0\rangle + \beta|1\rangle$.

Their inner product is α .

Linearity upper bounds the probability that these states would behave differently when something – anything at all – is done to them. With probability at least $\alpha^* \alpha$ they'll behave identically.

This is a huge difference from ‘classical’ physics, where points in phase space are arbitrarily distinguishable.

Uncertainty

Different observables won't commute – their eigenstates are nonorthogonal.

Measurement disturbance

Preparing an eigenstate of one observable overwrites information about other observables.

No cloning of quantum information

Quantum states cannot be copied.

If they could, we could measure any observable without disturbance simply by creating clones and studying them.

Quantum cloning machine

if $|0\rangle|x\rangle \longrightarrow |0\rangle|0\rangle$

and $|1\rangle|x\rangle \longrightarrow |1\rangle|1\rangle$

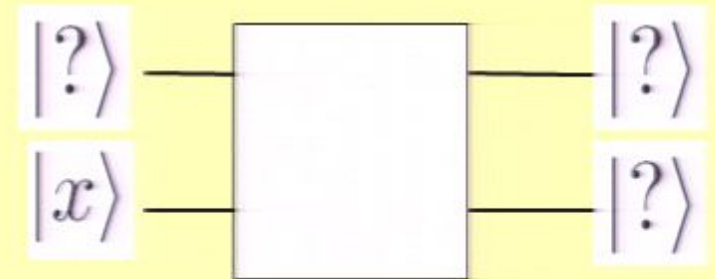
Then by linearity...

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|x\rangle \longrightarrow \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$$

But we wanted a different state:

So linearity has thwarted us!

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$



No deleting of quantum information

Quantum states cannot be deleted either! ...assuming no wavefunction collapse.

The closest we can come is diffusing away the information as correlations with a large environment.

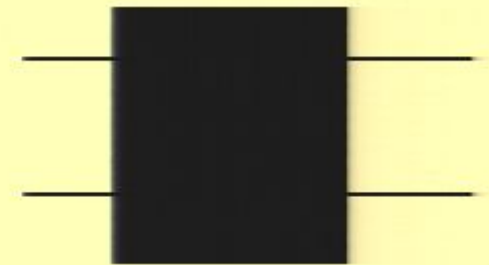
Quantum deleting machine

$$|\psi\rangle|\psi\rangle \longrightarrow |\psi\rangle|0\rangle$$

But this is only possible in general if the state is swapped into the environment, to survive forever.

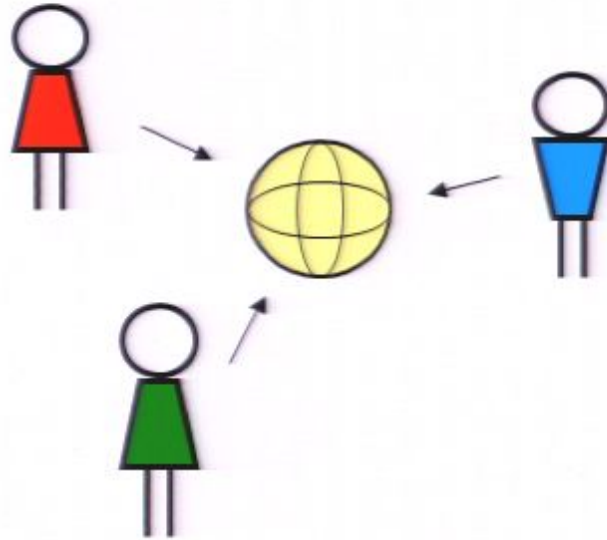
$$|\psi\rangle|\psi\rangle|E\rangle_E \longrightarrow |\psi\rangle|0\rangle|E'\rangle_E$$

It may, however, be stored as highly entangled correlations amongst many parts of the environment, putting it out of reach, if not out of existence.



Quantum information

Quantum information is hard to hold onto. If several people want to get quantum information from a system, they can only do so at each others' expense.

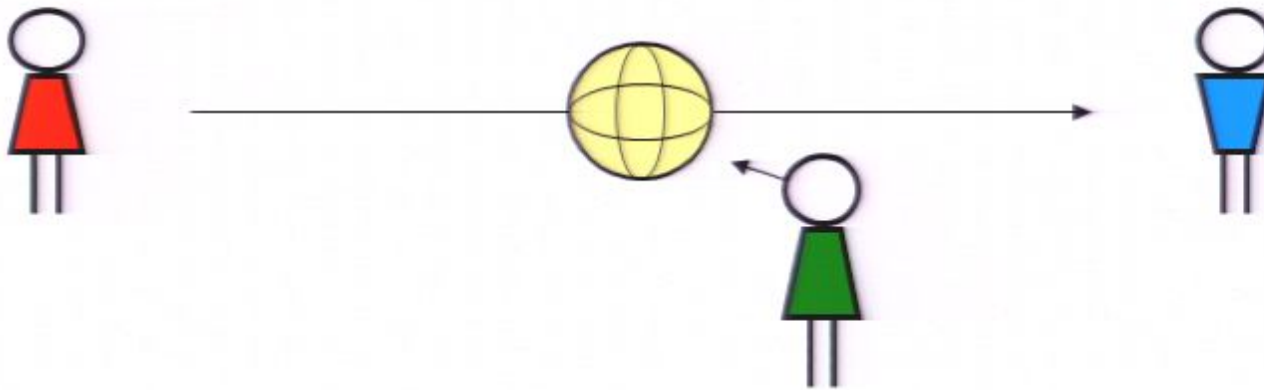


If the environment becomes correlated with your system, you lose information. (It moves from being locally stored in your system, which you could access, to being stored in correlations with the environment, which you probably can't.)

This is a big practical problem for people building quantum information devices – how to keep noise to a minimum. But it's also a source of strength...

Quantum cryptography

Information is physical, so gaining and losing it has noticeable physical consequences.



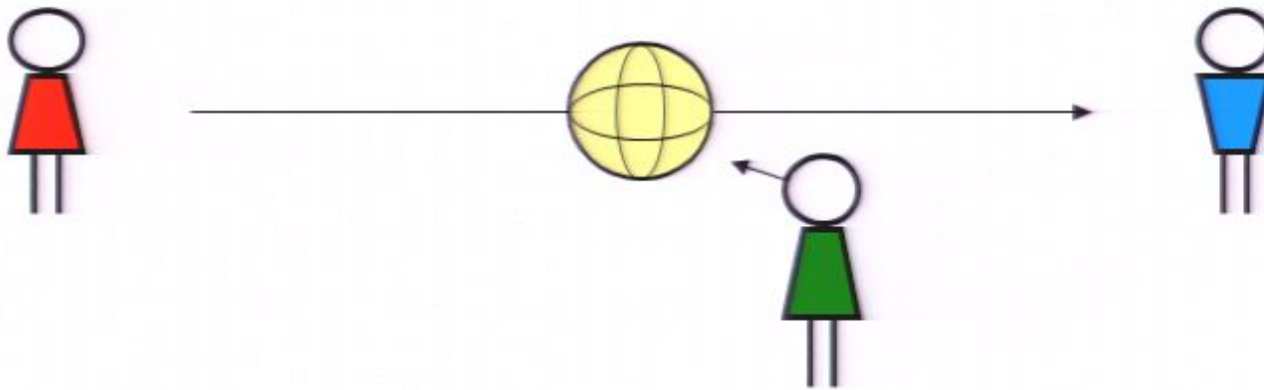
Suppose Alice is sending some quantum information to Bob. If Eve intercepts it, Bob won't get the information.

Eve can send replacement signals to deceive Bob, but when he checks with Alice, he'll find out those replacement signals don't match what she sent.

Eve can't forward an accurate copy of the information to Bob, because she can't copy it!

Quantum cryptography

Eve does get the message, though, if she wants...



...but if that message was establishing a shared private key for one-time pad cryptography, this doesn't matter too much. Alice and Bob detect Eve's malign presence and abort before they send any ciphertext to one another.

Alice and Bob can create a 'physically secure' communication channel.

Quantum cryptography



MagiQ™

id Quantique
A Quantum Leap For Cryptography

Quantum cryptography

(21st April 2004)

QBanking - Bank - Received Transaction at 12:07:48

**Bank Austria
Creditanstalt**

ÜBERWEISUNG - INLAND


EUR		Betrag	3000.00
Kontonummer - EmpfängerIn	BLZ - Empfängerbank	Empfängerbank	
00290620400	12000	BA-CA	
EmpfängerIn UNIVERSITÄT-WIEN			
Unterschrift AuftraggeberIn - bei Verwendung als Überweisungsauftrag		Verwendungszweck	
		Spende an Institut für Experimental- physik	
Kontonummer - AuftraggeberIn	BLZ-Auftragg./Bankverm.		
51381381781	12000		
AuftraggeberIn/EinzahlerIn - Name und Anschrift			
Bob Havelka			

Quantum Experiments and the Foundations of Physics
Prof. Anton Zeilinger

seibersdorf research
an IBM Research Center

UNIVERSITÄT WIEN

**Bank Austria
Creditanstalt**

 **Stadt Wien**

Entanglement

If $|00\rangle$ and $|11\rangle$ are pure states, so is: $\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$

Entangled states are fundamentally different from classical mixtures:

Classical Mixture

$$P^{(1/2)} = |00\rangle \quad P^{(1/2)} = |11\rangle$$

$$\frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$ZZ \rightarrow \frac{1}{2} (+1, +1); \frac{1}{2} (-1, -1).$$

$$XX \rightarrow \frac{1}{4} (+1, +1); \frac{1}{4} (-1, +1);$$

$$\frac{1}{4} (+1, -1); \frac{1}{4} (-1, -1).$$

Pure Entangled State

$$|0\rangle|0\rangle + |1\rangle|1\rangle$$

$$\frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

$$ZZ \rightarrow \frac{1}{2} (+1, +1); \frac{1}{2} (-1, -1).$$

$$XX \rightarrow \frac{1}{2} (+1, +1); \frac{1}{2} (-1, -1).$$

Entanglement



Classical correlations at a distance are possible (e.g. socks). QM allows stronger correlations over a broader range of possible measurements on each system.

Entanglement comes at the expense of *local information*. If the overall system is in a maximally entangled state:

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

The local systems A and B are described by maximally mixed states:

$$\rho_a = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \quad \rho_b = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$$

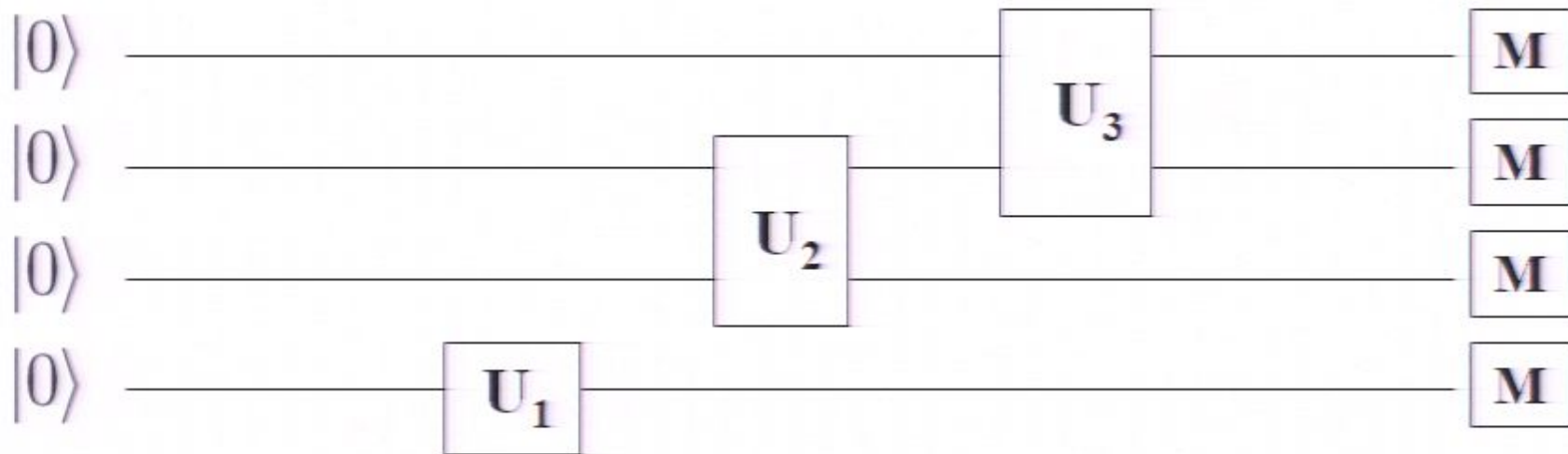
Local behaviour is entirely unpredictable. The entangled state contains *only* global information.

We can measure global properties of systems directly...without paying the cost of finding local properties.

Quantum computation

‘Computation’ means computing functions: $f(\text{input}) = \text{output}$.

Quantum computers can be built with analogous architecture to classical ones:



- Register of inputs, all in a default state.
- One and two qubit unitary operations (=logic gates). This is universal.
- Outputs, which can be measured in the $\{0,1\}$ basis.

Quantum computation

Suppose we have a black box that computes a one-qubit function:



That function can have one of two properties:

constant : $f(0) = f(1)$

balanced: $f(0)$ is not $f(1)$

How many queries do we need to discover this property?

Classically, we need two. We can only find it by exhaustively learning f .

Quantumly, we need one.

Deutsch's algorithm

$$|01\rangle$$

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

constant

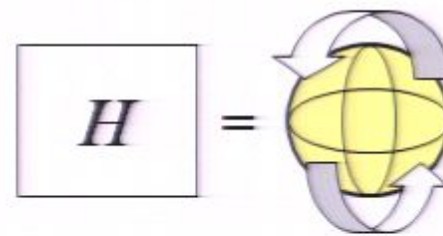
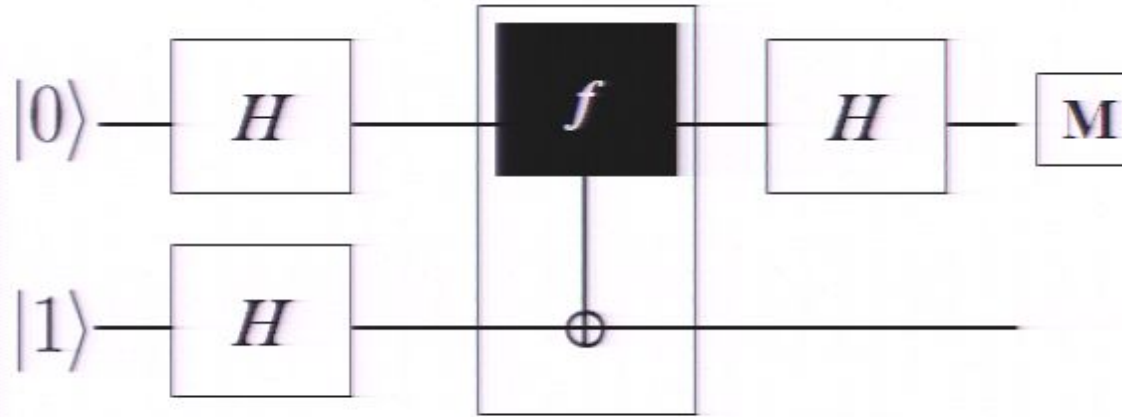
balanced

$$(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$$

$$\frac{1}{2}(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$$

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

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



$$|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$



$$= |x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$$

In one shot, we output a bit: $|0\rangle$ if f is constant and $|1\rangle$ if f is balanced.

Shor's algorithm

A 2-to-1 speedup is not that impressive, but it can scale!

A more famous problem, and one without a black box, is factoring:

Let x be a large integer. Find the prime factors of x .

Classically, this is so hard that it forms the basis of most cryptography (e.g. RSA).

As x gets larger, the length of time it takes to find its factors grows exponentially.

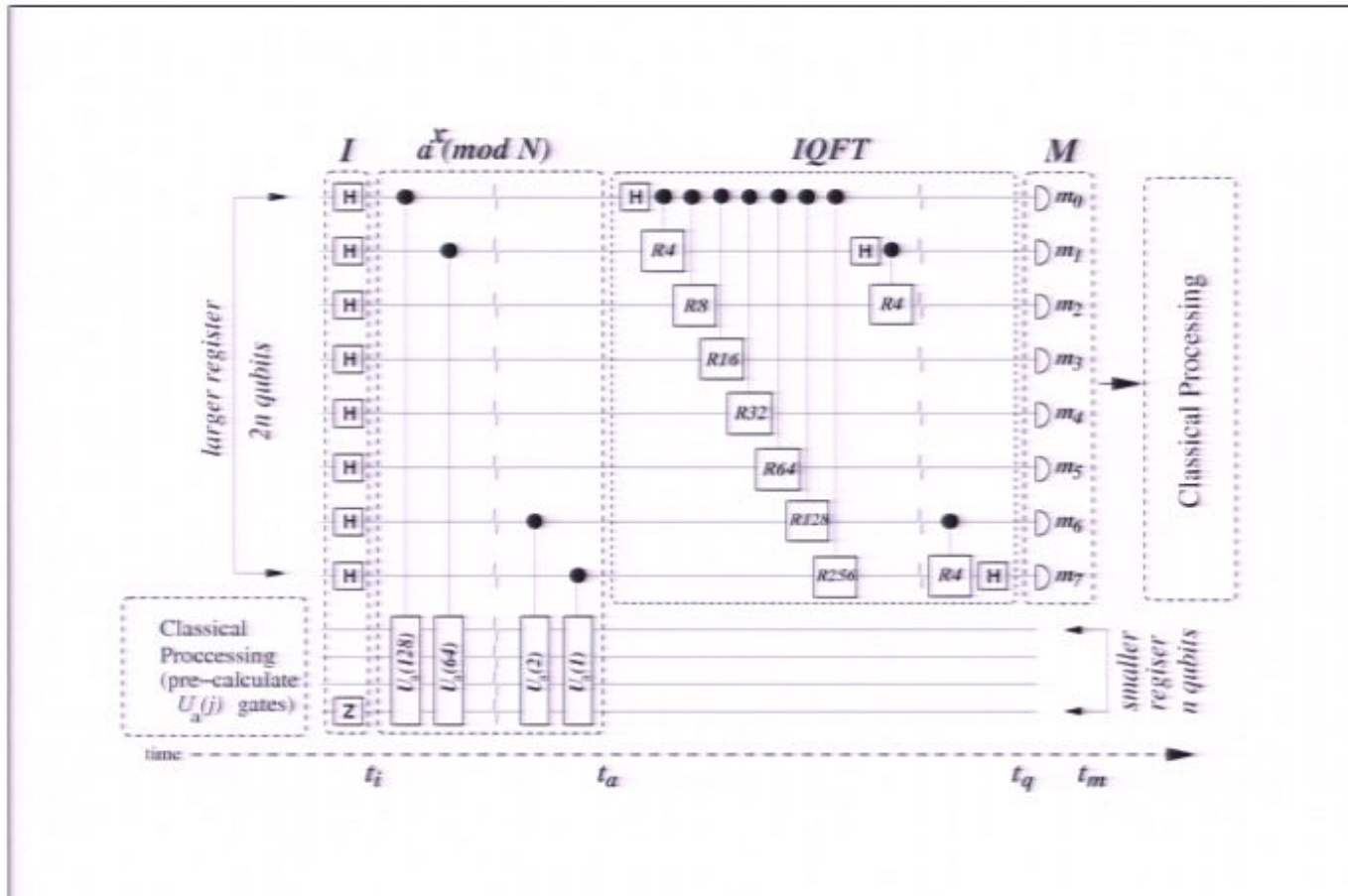
It reduces to the problem of period finding.

Let $f(x)$ be a periodic function on the integers such that $f(x+a)=f(x)$ for some a . Find a .

a can be very large. The best classical techniques for finding these periods are not much better than guesswork.

A quantum fourier transform circuit can find a efficiently - in $O[(\ln n)^3]$.

Shor's algorithm



$3 \times 5 = 15$, Lieven et al., *Nature* 414

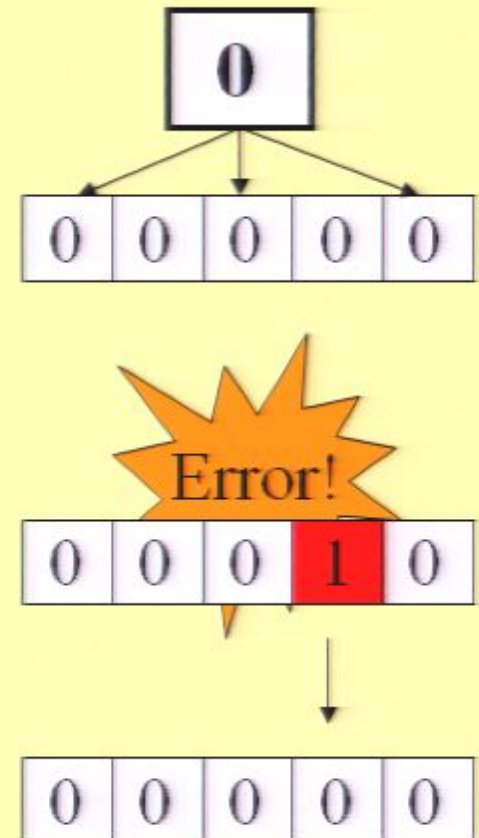
Yes yes, but it won't work in practice...

“Quantum computation may work in theory, but won't any accumulation of noise destroy the information being processed?”

Actually, no. Sure, quantum information is fragile, but we can protect it!

Classical error correction vs. bit flips.

1. Encode the logical bit '0' as 00000, ('1' as 11111).
2. An error occurs with probability p .
For small enough p , one error is much more likely (p) than at least four ($O(p^4)$).
3. Since the 0's are in the majority, we correct to 00000.



Quantum error correction

Quantum error correction vs. Pauli errors.

1. Encode the quantum states $|0\rangle$ and $|1\rangle$ as carefully chosen entangled states (codewords) of five qubits.

2. An Pauli error occurs with probability p .

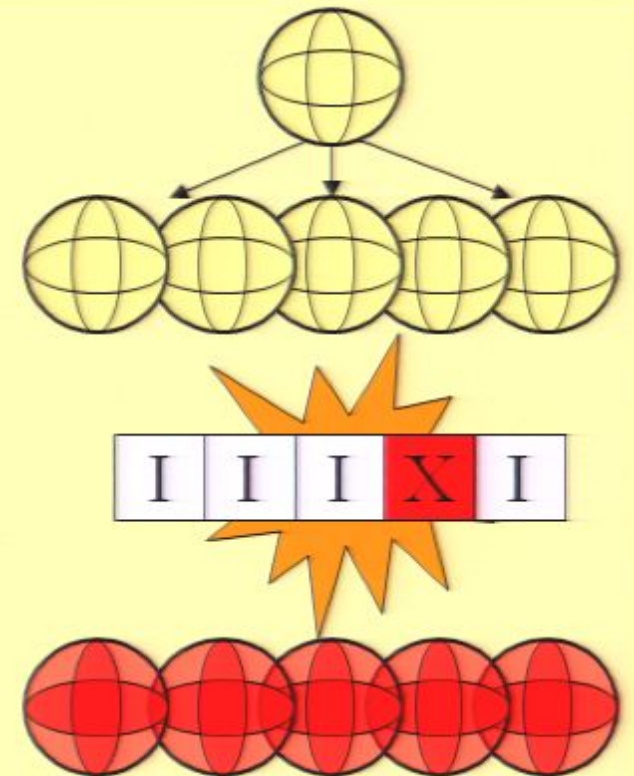
We're moved from one state to another.

But there are 15 possible Pauli errors (3x5).

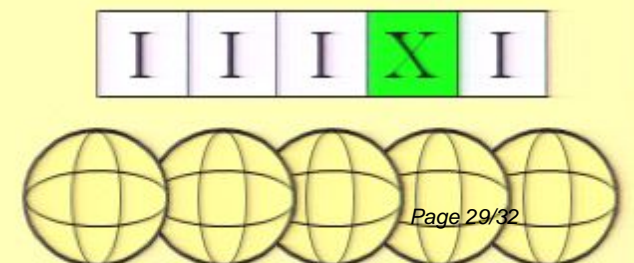
All states at most one Pauli distant from the initial state lie within a 16 dimensional subspace.

All 32 error states are orthogonal!

So we can deterministically work out which error occurred, and reverse it!



Measurement reports "X4"



Quantum error correction

Quantum error correction vs. general errors.

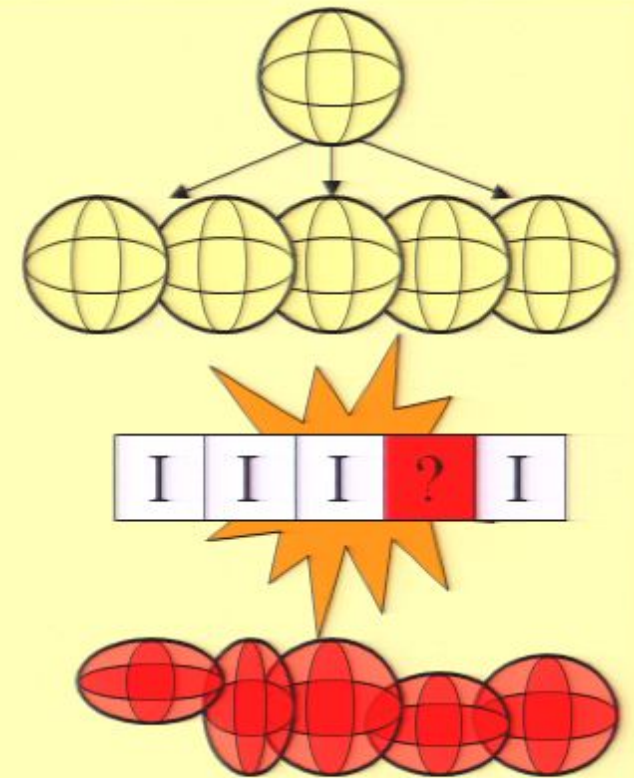
The same protocol also solves general errors.

The measurement step imposes Pauli errors...

...and disentangles the system from the environment!

General error remains unknown...

...but we only have to correct the Pauli error we replaced it with!



Measurement reports "X4"

I I I X I



Fault tolerance

Error correction is not enough to compute with noisy gates and data, since:

- Gates might actively propagate errors.
- Error correction operations might be faulty.

However, even with noisy qubits, noisy gate operations, imprecise measurements and imperfect error correction, we can still quantum compute reliably!

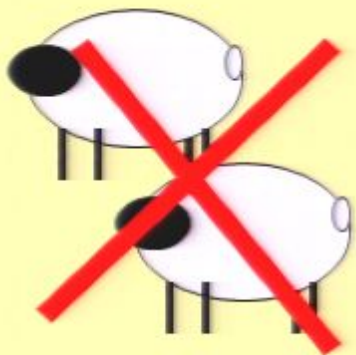
1. Design gates and such that $p(2 \text{ errors coming out})$ is $O(p^2)$.
2. Get p below a finite threshold.
3. Profit! Arbitrarily large quantum computations.

How low is the threshold? That depends.....

Quantum information theory

Quantum mechanics is *really* about the properties of physical information.

- Probabilities, expectations, etc...
- Operational language – measurements, transformations, outcomes.



No cloning



Teleportation



Q Cryptography



Q Cryptanalysis