What is Quantum Information and Technology?

Prof. Ivan H. Deutsch
Dept. of Physics and Astronomy
University of New Mexico

Second Biannual Student Summer Retreat of the SQuInT Network

St. John's College, Santa Fe, New Mexico
June 25, 2001 – June 29, 2001

Outline

- What is **classical information**?
- What is **quantum information**?
- What is **quantum computing**?
- How would we **implement** these ideas?

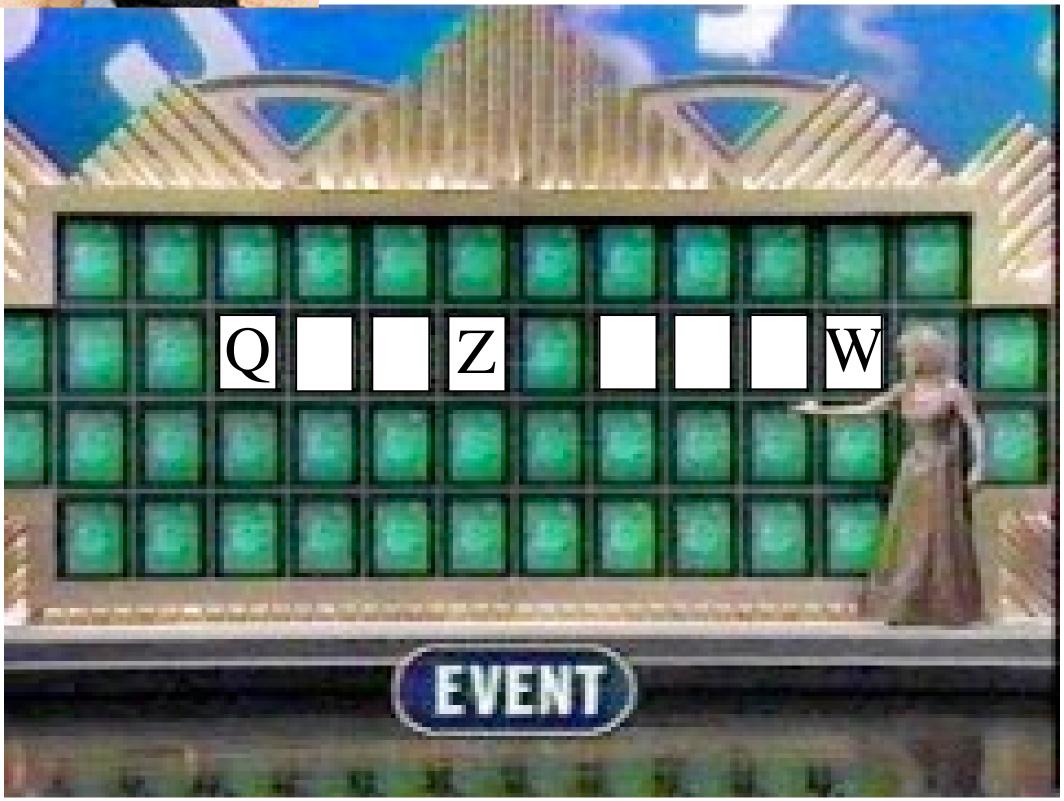
References:

- M. A. Nielsen and I. Chuang, *Quantum computation and quantum information"* (Cambridge Press, 2000).
- Prof. Preskill's notes: http://www.theory.caltech.edu/people/preskill/ph229/
- *Introduction to Quantum Computation and Information*, H-K Lo, S. Popescu, T. Splliller eds., (World Scientific, 1998).
- Special Issue of Physical Implementations: Fortschritte der Physik **48** 2000.


WHEEL OF FORTUNE


U I O
EVENT


WHEEL OF FORTUNE


Q
Z
W
EVENT

Quantifying Information

3 bit message: {000, 001, 010, 011, 100, 101, 110, 111}

With no *prior knowledge*:

$$Information = \log_2(\#\text{ of possibities}) = \log_2(8) = 3 \text{ bits}$$

With *a priori knowledge (probabilistic)*:

Probability 0 = p
Probability 1 = 1-p

- "Typical word" of length N has: Np 0's and N(1-p) 1's
- $$\#_{typ} = \binom{N}{Np} = \frac{N!}{(Np)!\left[N(1-p)\right]!}$$
- Information in a typical word = $\log_2(\#_{typ})$

Shanon Information

Shanon Information = ***Average information/ letter***

$$H(p) = \frac{\log_2(\#_{typ})}{N} = -p\log_2(p) - (1-p)\log_2(1-p)$$

(Sterling's approximation: $\log(N!) \approx N\log N - N$)

Generally, given alphabet: $\{a_j \mid j = 1,..,n\}$ with probability p_j

$$H(A) = -\sum_{j=1}^{n} p_j \log_2(p_j) = \textbf{\textit{Entropy}}$$

$-\log_2(p_j) =$ Information in a_j

$0 \le H(A) \le \log_2(n)$

Mutual Information

Suppose: Alice send message ***A*** with probability ***p(A)***

Bob receives message ***B*** with probability ***p(B)***

How much information can Alice communicate to Bob?

Degree of correlation: $p(A;B) = p(A)p(B) \div p(A,B)$

Joint probability

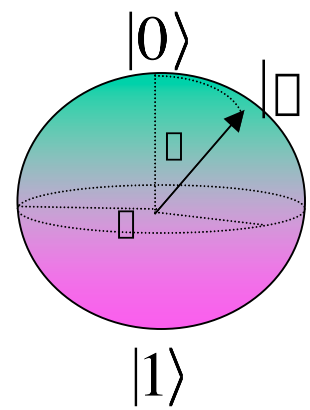
$$I(A;B) = \langle -\log(p(A;B)) \rangle = I(B;A)$$

- **Information Bob gets from Alice**
- **Information common to *A* and *B***

Quantum Information

Information encoded in a *quantum state*, $|\psi\rangle$, more generally ρ.

Qubit: Two-level quantum system



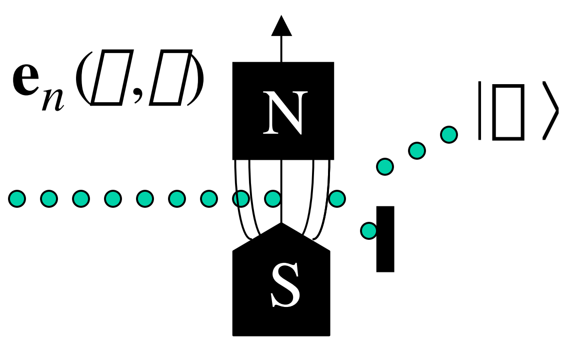
$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle$

$\{|0\rangle, |1\rangle\}$
"Logical Basis"

Bloch sphere

Tremendous amount of information ***encoded*** in $|\psi\rangle$

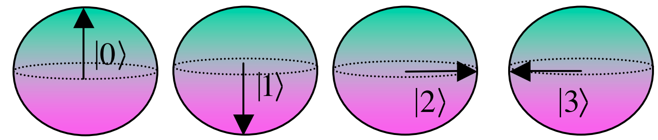
$\mathbf{e}_n(\theta,\varphi)$



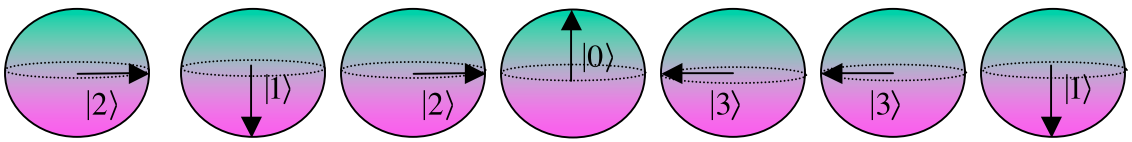
Given finite precision to specify θ,φ Alice can specify *many* different $|\psi\rangle$

Inaccessible Information

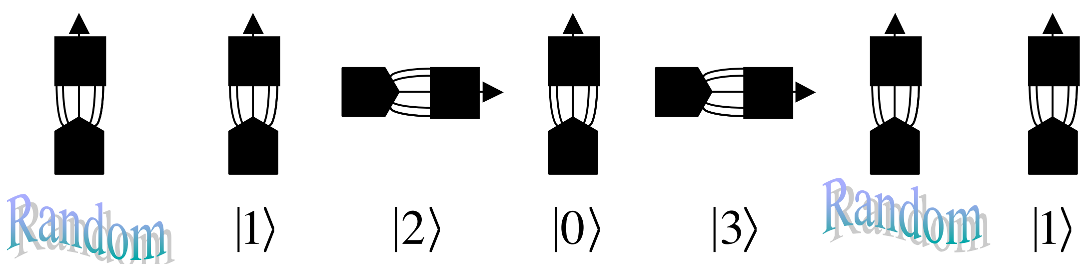
- Alice encodes 2 " classical bit" in a qubit



<u>Message</u>



- Bob decodes through Stern-Gerlach apparatus.

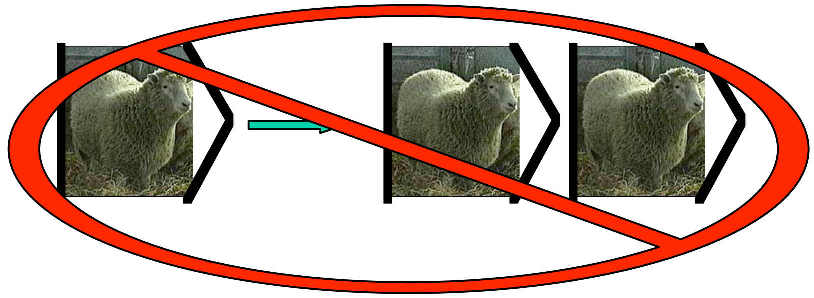


Quantum information ***cannot be read***

Holevo Bound
Alice cannot send more than one bit of information to Bob per qubit!

$$I(A;B) \leq 1 \text{ bit}$$

No Cloning



Suppose Bob wants to be cleaver and make many copies of $|\psi\rangle$.

$$|\psi\rangle \rightarrow |\psi\rangle|\psi\rangle|\psi\rangle|\psi\rangle|\psi\rangle|\psi\rangle$$

e.g. copy the unknown qubit onto an "ancilla" qubit $|\psi\rangle|0\rangle \rightarrow |\psi\rangle|\psi\rangle$

- Transformation on basis states

$$|0\rangle|0\rangle \rightarrow |0\rangle|0\rangle \qquad |1\rangle|0\rangle \rightarrow |1\rangle|1\rangle$$

- ***Linearity***

$$(\alpha|0\rangle + \beta|1\rangle)|0\rangle = \alpha|0\rangle|0\rangle + \beta|1\rangle|0\rangle \rightarrow$$

$$\alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle \neq (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)$$

Quantum Information cannot be copied!

Information Gain ⇒ *Disturbance*

Attempt to copy “distinguishing information” into an ancilla.

$$|\psi\rangle|u\rangle \to |\psi\rangle|v\rangle \qquad |\varphi\rangle|u\rangle \to |\varphi\rangle|v'\rangle$$

$$(\langle\varphi|\langle u|)(|\psi\rangle|u\rangle) = (\langle\varphi|\langle v'|)(|\psi\rangle|v\rangle)$$

$$\langle\varphi|\psi\rangle = \langle\varphi|\psi\rangle\langle v'|v\rangle$$

$$\text{If } \langle\varphi|\psi\rangle \neq 0 \;\Rightarrow\; 1 = \langle v'|v\rangle$$

Any attempt to distinguish between two ***non-orthogonal*** states necessarily results in a disturbance of the states

Composite Systems

Classical

- One bit: $A=\{a \mid a=0 \text{ or } 1\}$
- Two bits: $A \otimes B = \{(a,b) \mid a,b = 0 \text{ or} 1\}$ ***Cartesian product***
- N bits: Space has 2^N configurations.

Quantum

- One qubit:

$$A = \{|\psi\rangle,\ |\psi\rangle = c_0|0\rangle + c_1|1\rangle,\ \ c_0, c_1 \text{ finite precision complex numbers}\}$$

- Two qubits: ***Tensor product***

$$A \otimes B = \{|\psi\rangle_{AB} = c_{00}|0,0\rangle + c_{01}|0,1\rangle + c_{10}|1,0\rangle + c_{11}|1,1\rangle\}$$

- N qubits: Space has $(2^x)^{2^N}$ states, with x bits for each c.

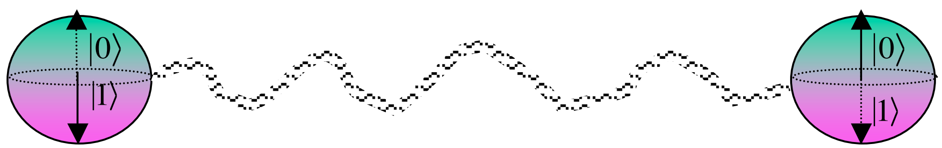
Expontenial growth in state space

Entanglement

(Pure) states *N*-qubits are generally "*entangled*"

$$|\psi\rangle \neq |\psi\rangle_1 \otimes |\psi\rangle_2 \otimes \cdots \otimes |\psi\rangle_N$$

→ ***Nonclassical correlations***
e.g. Two qubits, Bell's Inequalities



$$|\Psi^{(-)}\rangle = \left(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B\right)/\sqrt{2}$$

Alice receives a random bit

Bob receives a random bit

Alice and Bob cannot communicate even one bit

- **Quantum-Information cannot be read.**
- **Quantum-Information cannot be copied.**
- **Nonorthogonal states cannot be distinguished.**
- **Exponential growth in *inaccessible* information.**
- **Quantum correlations cannot be used for communicating classical information**
- **Measurement is *irreversible - collapse of the wave function*.**

Quantum Mechanics is a Nuisance?

Quantum Information as a Resource

Information-Gain/Disturbance:

- Quantum Cryptography - Secret key distribution

Tensor Structure of Composites (Entanglement)

- Quantum dense coding - Sending two classical bits with one classical bit plus EPR.
- Quantum teleportation - Communicating a qubit
- Quantum Computation

Elements of Quantum Computation

$$|\psi_{in}\rangle \longrightarrow \boxed{\hat{U}} \longrightarrow |\psi_{out}\rangle$$

Take advantage of exponentially large state space

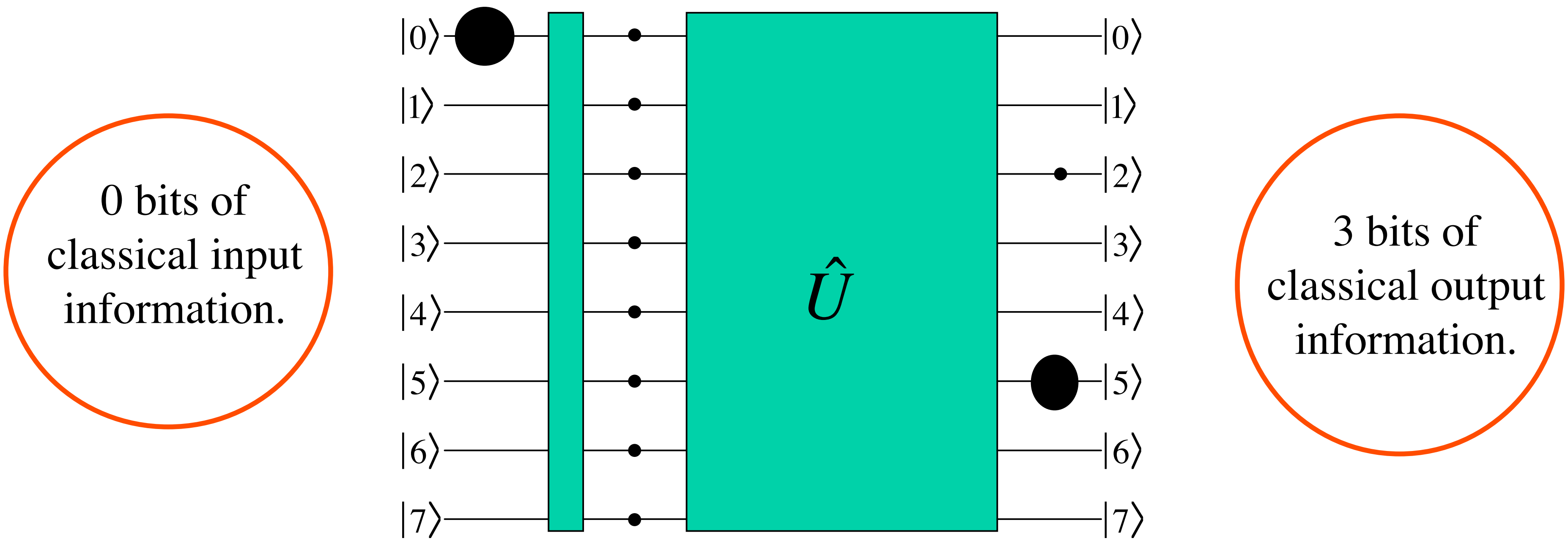
- ***Quantum Register:*** quantum state of the system
- ***Quantum Logic Gates:*** unitary transformation on subsystems
- ***Error-tempering:*** correct/suppress errors
- ***Measurement:*** read out classical information

Quantum Parallelism (Deutsch)

E.g. 3-qubit "quantum register"

$$|0\rangle = |0\rangle|0\rangle|0\rangle \quad |1\rangle = |0\rangle|0\rangle|1\rangle \quad |2\rangle = |0\rangle|1\rangle|0\rangle \quad |3\rangle = |0\rangle|1\rangle|1\rangle$$

$$|4\rangle = |1\rangle|0\rangle|0\rangle \quad |5\rangle = |1\rangle|0\rangle|1\rangle \quad |6\rangle = |1\rangle|1\rangle|0\rangle \quad |7\rangle = |1\rangle|1\rangle|1\rangle$$



Quantum Computer is a multiparticle Interferometer

Quantum Computing: Quantum Control in Asymptopia

$$|\square_{in}\rangle \longrightarrow \boxed{\hat{U}} \longrightarrow |\square_{out}\rangle$$

$$|\square\rangle \equiv \textit{Many-body State}$$

Complexity: *Asymptotic Behavior*

Given n bits to specify the state, how do the resources scale as n | |

Resources:

- Time
- Energy
- Space

- "***Easy***" Polynomial in *n*
- "***Hard***" Exponential in *n*

Quantum Logic Gates

- **Single qubit:**

$$U = \sum_{i=0}^{3} c_i \sigma_i, \quad \sum |c_i|^2 = 1$$

$$\sigma_0 = 1, \quad \sigma_{i=1,2,3} = \text{Pauli}$$

Rotation on Bloch sphere

NOT: $\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\quad |0\rangle \to |1\rangle$, $\quad |1\rangle \to |0\rangle$

Hadamard: $H = \dfrac{\sigma_1 + \sigma_3}{\sqrt{2}}$ $\quad |0\rangle \to (|0\rangle + |1\rangle)/\sqrt{2}$, $\quad |1\rangle \to (|0\rangle - |1\rangle)/\sqrt{2}$

- **Two qubit:**

$$U = \sum_{i,j} c_{ij}\, \sigma_i^{(1)} \sigma_j^{(2)}$$

"Entangling unitary"

Controlled NOT: $|x\rangle|y\rangle \to |x\rangle|x \oplus y\rangle$

Control Target

$|0\rangle|0\rangle \to |0\rangle|0\rangle$

$|0\rangle|1\rangle \to |0\rangle|1\rangle$

$|1\rangle|0\rangle \to |1\rangle|1\rangle$

$|1\rangle|1\rangle \to |1\rangle|0\rangle$

Flip the state of the target bit conditonal on the state of the control bit $\quad \sigma_3 \quad \sigma_1$

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

Universality

• <u>Logic Gates:</u> Basic building blocks

$\hat{U}: \mathrm{H} \equiv \Box\, a_{i_1 i_2 \cdots i_N} \Box_{i_1} \quad \Box_{i_2} \quad \cdots \quad \Box_{i_N}$

Unitary acts on combinations of qubits

Universal Logic Gates

$\left\{ R_{\mathbf{e}_n}(\Box);\ \ cNOT \right\}$

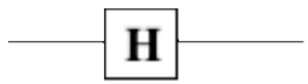
Single qubit rotation

Two-qubit entangling gate

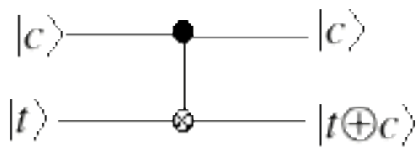
Entangling Gate: $\hat{H}_{12} \neq \hat{H}_1 + \hat{H}_2$ Nonseparable

Efficient algorithms: # of gates not exponential in N

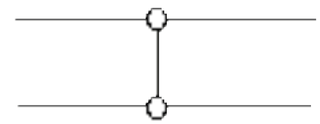
Quantum Circuits



Hadamard

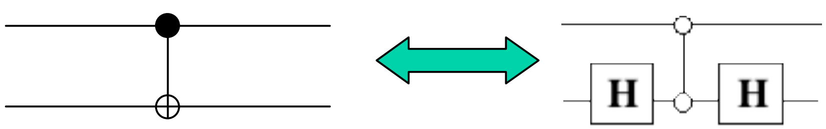


CNOT

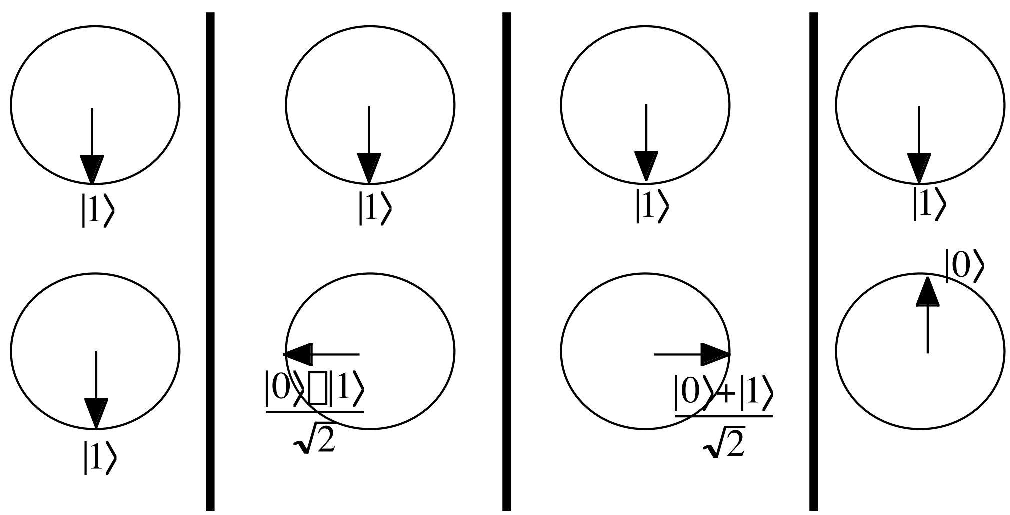


CPHASE

$$|0\rangle|0\rangle \to |0\rangle|0\rangle$$
$$|0\rangle|1\rangle \to |0\rangle|1\rangle$$
$$|1\rangle|0\rangle \to |1\rangle|0\rangle$$
$$|1\rangle|1\rangle \to -|1\rangle|1\rangle$$



CNOT from CPHASE



(I) **(II)** **(III)** **(IV)**

Deutsch's Problem

- **Problem:** Given function with two inputs and outputs

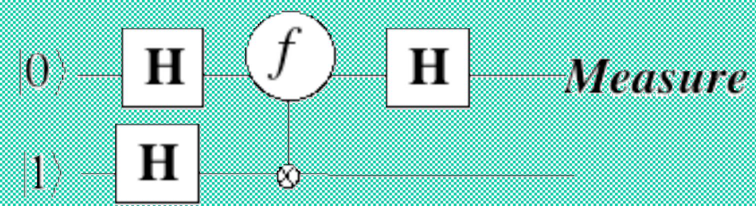
$$f:\{0,1\}\rightarrow\{0,1\} \quad \text{is} \quad f(0)=f(1)\ ?$$

- **Classical solution - requires TWO calls of *f***
- **Quantum solution - requires ONE call of *f***

Quantum function evaluation

$$\hat{U}_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle$$

REVERSABLE



$$|0\rangle|1\rangle \Rightarrow \left(|0\rangle+|1\rangle\right)\left(|0\rangle-|1\rangle\right) = \left(|0\rangle\left(|0\rangle-|1\rangle\right)+|1\rangle\left(|0\rangle-|1\rangle\right)\right)$$

$$\Rightarrow (-1)^{f(0)}|0\rangle\left(|0\rangle-|1\rangle\right)+(-1)^{f(1)}|1\rangle\left(|0\rangle-|1\rangle\right)$$

$$=\left(|0\rangle+(-1)^{f(1)-f(0)}|1\rangle\right)\left(|0\rangle-|1\rangle\right)$$

$$\Rightarrow |0\rangle\left(|0\rangle-|1\rangle\right) \qquad \textbf{\textit{OR}} \qquad \Rightarrow |1\rangle\left(|0\rangle-|1\rangle\right)$$

(f constant) ***(f balanced)***

The Tao of Quantum Computation

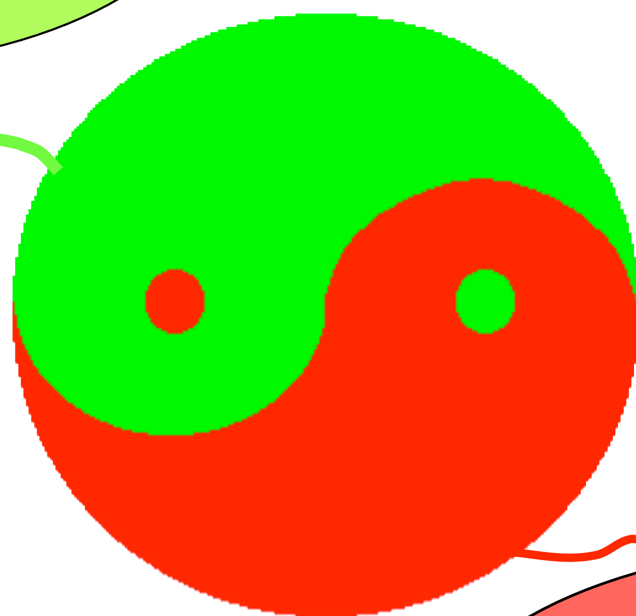
Coupling Between Qubits

- Entanglement

Coupling To External Drive

- Unitary evolution

Coherence



Decoherence

Coupling to the Environment

Errors

Physical Implementations

Atomic-Molecular Optical Systems (Gas Phase)

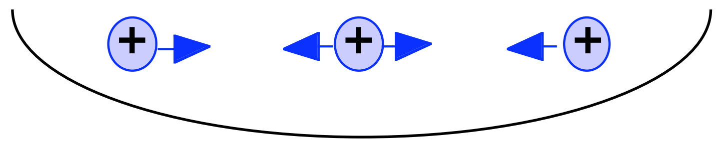
- Ion Traps
- Cavity *QED*
- Neutral Atom Traps
- Linear/Nonlinear Optics

Condensed Matter (Liquid or Solid Phase)

- Semiconductors (electronics)
- Nuclear/Electron Magnetic Resonance (liquid, solid, spintronics)
- Superconductors (flux or charge qubits)
- Electrons floating on liquid helium

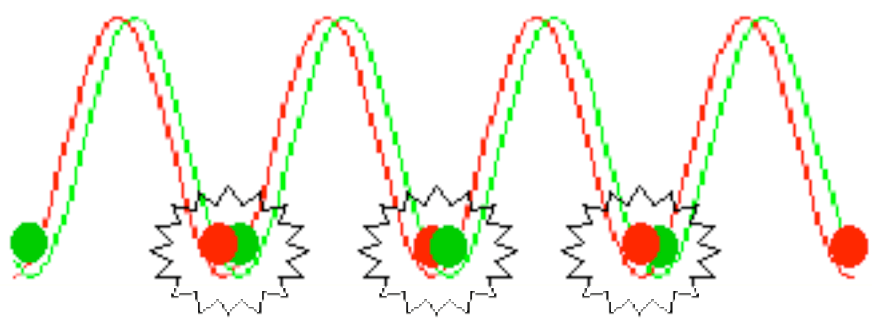
Electric Monopole

- **Ion Trap**



- **Strong Qubit Coupling: Coulomb Repulsion**
- **Strong Coupling to Environment - Technical Noise**

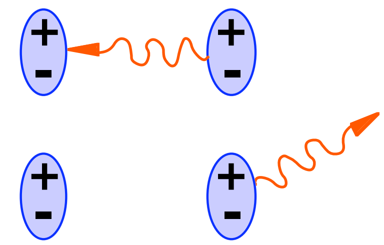
- **Neutral atom trap (optical lattice)**



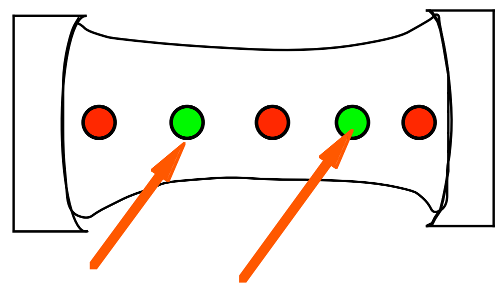
- **Strong Qubit Coupling "On demand:** ***elastic collision***
- **Coupling to Environment -** ***inelastic collision***

Electric Dipole-Dipole

- Coherent photon exchange
- Spontaneous emission

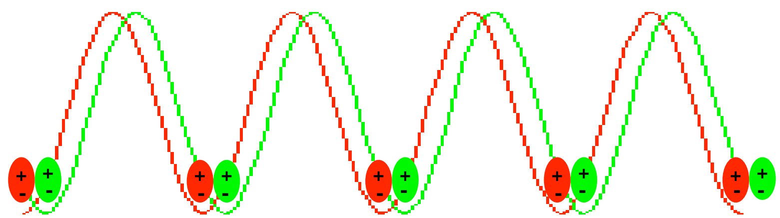


Cavity QED:



- Interactions turned “on” and “off”
- Real photon exchange
- Strong-coupling regime (enhance coherence)

Optical Lattice:



- Virtual photon exchange
- Near-field interaction dominates

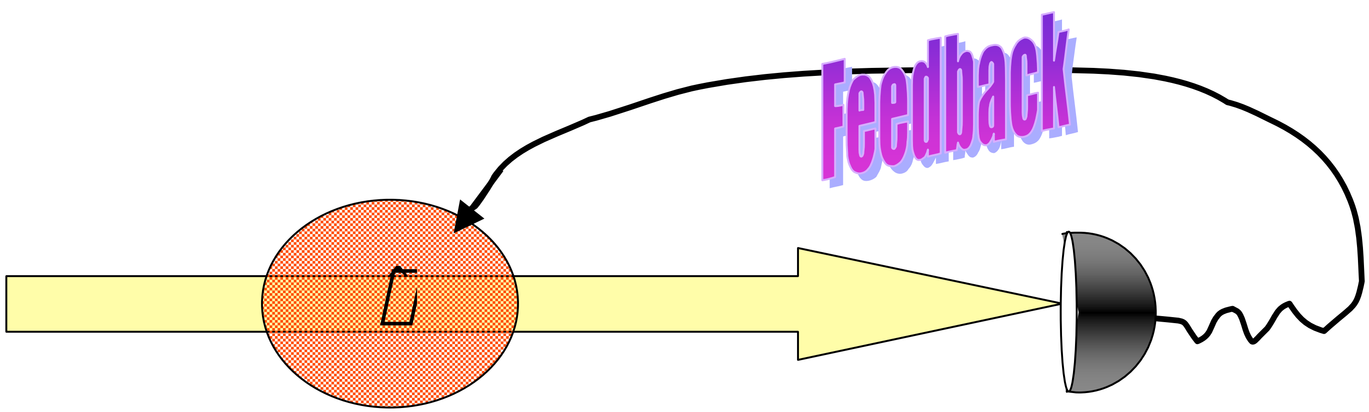
Measurement

Ideal: $|\psi_{in}\rangle$ → $\hat{U}$ → $|\psi_{out}\rangle$

Reality: $\hat{\rho}_{in}$ → **$** → $\hat{\rho}_{out}$

$$\$[\hat{\rho}] = \sum_j \hat{A}_j \hat{\rho} \hat{A}_j^\dagger$$

$$\sum_j \hat{A}_j^\dagger \hat{A}_j = 1$$



Summary

- Information Processing constrained by ***physical laws***.
- Quantum Information:
  - **Information-gain/disturbance.**
  - **Exponential growth of state space. Entanglement.**
- Quantum Computation - asymptotic savings of ***physical resources***.
- Physical Implementation - *Quantum Control of Many-body System!*

Classical Physics

Digital: Particles

Analog: Waves

→

Quantum Physics

Waveparticle

Duality