An Introduction to
Quantum Information

by Carl J. Williams
National Institute of Standards & Technology

http://qubit.nist.gov

MCSD Seminar -- NIST
March 23, 2004
# Table of Contents

## I. What is Quantum Information? 4

## II. Introduction 6

- A. 20th Century in Review 7
- B. History of Quantum Information 9
- C. Uses of Quantum Information? 10
- D. Scaling of Quantum Information 11

## III. The Quantum Primer – (hard, but necessary) 12

- A. Schrödinger Equation and Dirac Notation 14
- B. Quantum Bits, Superposition, and the Bloch Sphere 21
- C. Quantum Observables, Projectors, and Measurement 25
- D. Wave vs. Particle Properties and Quantum Interference 28
- E. Quantum Entanglement and Multiple Quantum Bits 32

## IV. Classical Bits vs. Quantum Bits 38

- A. Scaling of Quantum Information Revisited 39
- B. Analog vs. Quantum Computing 41
- C. Quantum Entanglement and Einstein-Podolsky-Rosen Paradox 42
- D. Quantum Circuits and the No Cloning Theorem 43
- E. Possible Applications of Quantum Information 49
Table of Contents – cont’d

V. Quantum Communication - 100% physically secure 50
   A. Quantum cryptographic key exchange: eg. BB84 Protocol 53
   B. Quantum Teleportation 57
   C. State of the Art in Quantum Communication 59
   D. Technology from Single Photon Sources and Detectors 63
   E. Schematic of a Quantum Communication System 70
   F. Is Quantum Communication Here? 76

VI. Quantum Computing 77
   A. Status of Quantum Algorithms including Shor’s Algorithm 81
   B. Universal Quantum Logic 82
   C. Quantum Error Correction 86
   D. Shor’s Algorithm 87
   E. Proposed Experimental Schemes 89
   F. The DiVincenzo Criteria for Quantum Computing 92
   G. Scalable Quantum Architectures 98

VII. Quantum Information Outlook and Impact 110

VIII. Conclusions 112
I. What is Quantum Information?

A radical departure in information technology, more fundamentally different from current IT than the digital computer is from the abacus.

A convergence of two of the 20th Century’s great revolutions

Quantum Mechanics
(i.e. atoms, photons, molecules)
“Matter”

Information
(i.e. books, data, pictures)
More abstract
Not necessarily material

A quantum computer if it existed could break all present-day public key encryption systems

Quantum encryption can defeat any computational attack
Quantum Information may be Inevitable

The limits of miniturization:

At atomic scale sizes quantum mechanics rules

– Since objects and electronic components continue to be miniaturized, inevitably we will reach feature sizes that are atomic in scale
– In general, attempts to make atomic-size circuits behave classically will fail due to their inability to dissipate heat and their quantum character

Thus quantum information may be inevitable!

Clearly, at the smallest scale, we need to take full advantage of quantum properties.

This emphasizes a different view of why quantum information is useful and also show why it may ultimately lead to quantum engineering.

Belief: Quantum Information and Quantum Engineering will have a tremendous economic impact in the 21st Century
“Using Shor’s quantum factorization algorithm, one can see that factoring a large number can be done by a QC – quantum computer – in a very small fraction of the time the same number would take using ordinary hardware. A problem that a SuperCray might labor over for a few million years can be done in seconds by my QC. So for a practical matter like code breaking, the QC is vastly superior.”

... 

“Wineland and Monroe worked out the single quantum gate by trapping beryllium ions. …”
At the beginning of the 20th century a series of crises had taken place in physics – the old physics (now called classical physics) predicted numerous absurdities. At first *ad hoc* fixes were made to the *classical* theory – but the theory became untenable.

In the 1920’s this crises gave way to a quantum mechanics – a new theory appropriate at the smallest scales (atomic, nuclear). Quantum mechanics reduces to classical physics under the appropriate conditions while removing the absurdities.

• **Foundations of Quantum Mechanics**
  – Planck: Planck’s Constant
  – Einstein: Photoelectric Effect, Light Quanta, Special Relativity, E=mc², General Relativity
  – deBroglie: Wave-Particle Duality
  – Heisenberg: Uncertainty Principle, Matrix Mechanics
  – Schrödinger: Wave Equation

Note – that Einstein, one of the fathers of quantum mechanics, died believing that quantum mechanics was incomplete.
Modern information theory originates in the 1930’s with the concept of a Turing machine capable of running a program or algorithm. The Church-Turing hypothesis then asserts that there exists an equivalent algorithm of similar complexity that can run on a Universal Turing Machine.

The discovery of the transistor in 1947, followed by integrated electronics, leads to the computer revolution and Moore’s law. In the late 1940’s, Shannon defines the concept of a unit of information, which is given physical limitations by Landauer.

- **Foundations of Information Theory**
  - Church-Turing: Computability, Universality
  - von Neumann: Concept of a computer
  - Bardeen, Brattain, & Shockley: Transistor
  - Shannon: Information Measures
  - Landauer: Physical Limitations of Information; explanation for Maxwell’s Demon
  - Bennett: Reversible Turing Machine
History of Quantum Information

• **Foundations**
  – Benioff: Quantum Turing Machine
  – Feynman, Deutsch: Concept of Quantum computation
  – Landauer, Zurek: Physics of information
  – Bennett, DiVincenzo, Ekert, Lloyd: Concept of Quantum information science
  – Shor: Q. Factoring and discrete log algorithm
  – Preskill, Shor, Gottesman, Steane: Quantum error correction, Fault tolerant QC
  – Lloyd: Quantum simulators and Universal QC

• **From Theory to Experiment**
  – Bennett, Gisin, Hughes: Demonstration of quantum cryptography
  – Wineland and Kimble: Demonstration of Qubits and quantum logic
How can we use Quantum Information?

• **Quantum Communication - 100% physically secure**
  – Quantum key distribution – generation of classical key material
  – Quantum Teleportation
  – Quantum Dense Coding

• **Universal Quantum Logic**: *all* quantum computations – *i.e. any arbitrary unitary operations* – may be efficiently constructed from 1- and 2-qubit gates

• **Quantum Algorithms**
  – Factorization of large primes (Shor’s algorithm)
  – Searching large databases (Grover’s algorithm)
  – Quantum Fourier Transforms
  – Potential attack of NP problems
  – Simulation of large-scale quantum systems

• **Quantum Measurement – improved accuracy**
  – Heisenberg limit \( \propto \frac{1}{N} \) vs Shot-Noise limit \( \propto \frac{1}{\sqrt{N}} \)
  – Better Atomic Clocks

• **Quantum Engineering – specialized quantum devices**
Scaling of Quantum Information

• **Classically**, information stored in a bit register: a 3-bit register stores one number, from $0 – 7$.  
  
  \[
  \begin{array}{ccc}
  0 & 0 & 0 \\
  0 & 0 & 1 \\
  0 & 1 & 0 \\
  0 & 1 & 1 \\
  \end{array}
  \]

  e.g. \[010\]

  \[2^2 \quad 2^1 \quad 2^0\]

  • **Quantum mechanically**, a 3-qubit register can store all of these numbers in an arbitrary superposition:

  \[a|000\rangle + b|001\rangle + c|010\rangle + d|011\rangle + e|100\rangle + f|101\rangle + g|110\rangle + h|111\rangle\]

  \[|\ldots\rangle\]

  Dirac Notation for the quantum state vector

• **Result:**
  – Classical: one N-bit number
  – Quantum: $2^N$ (all possible) N-bit numbers
III. The Quantum Primer

- Schrödinger’s Equation and Dirac Notation
- Light as Waves and Photons
- Quantum Nature of Matter: Atoms
- Superposition
- Quantum Measurement
- Quantum Interference
- Entanglement
Quantum Theory Summary

Quantum theory is the branch of physics that describes waves and particles at the smallest scale and lowest energies. This theory is based on the observation that changes in the energy of atoms and molecules occurs in discrete quantities known as quanta. This includes the electromagnetic field which consists of individual quanta of various frequencies known as photons.

The classical or Newtonian limit (which describes everyday phenomena) is typically recovered when a complex quantum system consisting of many parts becomes massive and/or its energy becomes large (many quanta).

Non-relativistic quantum mechanics gives rise to Schrödinger’s wave equation. The key components of this equation, which in turn fully describes the system, are the Hamiltonian $H$ that governs the interactions of the quantum system and the wavefunction $\Psi(r,t)$ that describes the state or wavefunction of the system. The latter is often denoted by the ket $|\Psi(t)\rangle$. 

Schrödinger Equation

Schrödinger’s wave equation is a first order differential equation that describes the time evolution of a quantum system under a Hamiltonian $H$. The Hamiltonian $H$ is the operator equivalent of the total energy of the system which can be represented as the sum of the kinetic and potential energies of the system.

$$i\hbar \frac{\partial \Psi(\vec{r},t)}{\partial t} = H(\vec{r},t)\Psi(\vec{r},t) \quad \hbar \text{ is Planck's constant}$$

Probability of being at position $\vec{r}$ at time $t$ \hspace{1cm} $\rho(\vec{r},t) = \Psi^*(\vec{r},t)\Psi(\vec{r},t)$

Total integrated probability at time $t$ \hspace{1cm} $\left\langle \Psi(t)|\Psi(t)\right\rangle = \int \Psi^*(\vec{r},t)\Psi(\vec{r},t) \, d\vec{r} = \int \rho(\vec{r},t) \, d\vec{r}$

Note: In general one does not put arguments inside of bras $|\text{label}\rangle$. 

14
Schrödinger Equation (2)

The Hamiltonian $H$ for the system can typically be written as

$$H (\vec{r}, t) = -\frac{\hbar^2}{2m} \nabla^2 + V (\vec{r}, t)$$

where $m$ is the mass, $V (\vec{r}, t)$ is the potential, and the $\nabla^2$ in the kinetic energy term. Basically $H$ describes the quantum systems interactions.

If the potential $V$ is time independent with the result that $H$ is time independent, one obtains the time independent Schrödinger equation. This is a second-order partial differential equation sometimes referred to as an eigenvalue equation:

$$H \left| \Psi_E \right\rangle = E \left| \Psi_E \right\rangle$$

In general one does not need to know about transistors to understand classical computers. Similarly one does not need to know about $H$ to understand quantum computers.
Example: Schrödinger’s Equation

For a time independent problem, Schrödinger equation’s can be written:

\[ H \Psi_n = E_n \Psi_n \]

For the special case of a 1-dimensional harmonic oscillator, the Hamiltonian is given by:

\[
H(x) = -\frac{\hbar^2}{2m} \frac{d^2}{dx^2} + \frac{1}{2} m \omega^2 x^2
\]

\[
E_n = \left( n + 1/2 \right) \hbar \omega
\]

\[
\langle \xi | \Psi_n \rangle = \exp \left( -\xi^2 / 2 \right) H_n (\xi) \quad \text{where} \quad \xi = \sqrt{m \omega / \hbar} x
\]

where \(H_n(\xi)\) is a Hermite polynomial and \(\Psi_n\) satisfies:

\[
\langle \Psi_n | \Psi_k \rangle = \int_{-\infty}^{+\infty} \exp \left( -\xi^2 \right) H_n (\xi) H_k (\xi) d\xi = 2^n n! \sqrt{\pi} \delta_{nk}
\]
Normalized Wavefunctions

Convention in quantum mechanics is to use normalized wavefunctions since the total integrated density of a quantum system should be $1 - i.e.$

$$\|\Psi(t)\| = \left<\Psi(t)|\Psi(t)\right>^{1/2} = 1$$

Thus in the example from the previous page, a normalized $\Psi_n$ can be written as:

$$\left<\xi|\Psi_n\right> = \frac{2^{-n/2}}{\sqrt{n!}\sqrt{\pi}} \exp\left(-\xi^2 / 2\right) H_n(\xi)$$

So that $\left<\Psi_n|\Psi_k\right> = \delta_{nk}$

Moreover for any quantum system, the state kets $|\alpha\rangle$ and $|\beta\rangle$ represent the same quantum state if they differ only by a non-zero multiplicative constant

$$\lambda \in \mathbb{C} \quad |\alpha\rangle = \lambda |\beta\rangle$$
Dirac Notation

The elements, wavefunctions, eigenfunctions, or state vectors that are the solution of Schrödinger’s equation form an \textit{orthonormal} set. These state vectors are called ket vectors and are individually denoted as $\left| \text{label}_i \right>$ or $\left| i \right>$. The set of all such vectors $\{\left| i \right>\}$ span an abstract vector space referred to mathematically as the Hilbert Space $\mathbb{H}$.

A Hilbert Space $\mathbb{H}$ is very much like ordinary cartesian space $(x,y,z)$. The square-of-the-length $l$ of a vector from the origin $O$ to an arbitrary point $i$ given by the point $(x_i, y_i, z_i)$ is:

$$l^2 = x_i^2 + y_i^2 + z_i^2 = (x_i \ y_i \ z_i) \begin{pmatrix} x_i \\ y_i \\ z_i \end{pmatrix}$$

In Dirac notation and quantum mechanics one would label the state $\left| i \right>$ and the length-squared or inner product would be denoted:

$$l^2 = \langle i \left| i \right> \text{ or } l = \langle i \left| i \right>^{1/2}$$
Dirac Notation (2)

In normal cartesian space the unit vectors

\[ \hat{x} = (1 \ 0 \ 0), \quad \hat{y} = (0 \ 1 \ 0), \quad \text{and} \quad \hat{z} = (0 \ 0 \ 1) \]

form an orthonormal set that spans the space.

Orthonormal because:

\[ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = 1 \]

and

\[ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = 0 \]

or \[ \langle \hat{x} | \hat{x} \rangle = \langle \hat{y} | \hat{y} \rangle = \langle \hat{z} | \hat{z} \rangle = 1 \quad \text{and} \quad \langle \hat{x} | \hat{y} \rangle = \langle \hat{y} | \hat{x} \rangle = \langle \hat{x} | \hat{z} \rangle = \langle \hat{y} | \hat{z} \rangle = 0 \]

Spans the space because an arbitrary vector \( |u\rangle \) can be written:

\[ |u\rangle = a |\hat{x}\rangle + b |\hat{y}\rangle + c |\hat{z}\rangle \quad \text{and in normalized form} \quad |\hat{u}\rangle \text{ as:} \]

\[ |\hat{u}\rangle = \frac{a |\hat{x}\rangle + b |\hat{y}\rangle + c |\hat{z}\rangle}{\sqrt{a^2 + b^2 + c^2}} \]
Quantum Mechanics for Mathematicians

The wavefunctions (previously denoted $|\Psi\rangle$) and quantum bits or qubits that arise from quantum mechanics live in a Hilbert space $\mathcal{H}$ (which may be finite and in the specific case of a single qubit: 2-dimensional). A Hilbert space $\mathcal{H}$ is a vector space over the complex numbers with a complex valued inner product. A complex valued inner product is a map: $(-,-) : \mathcal{H} \times \mathcal{H}^\text{op} \rightarrow \mathbb{C}$ from $\mathcal{H} \times \mathcal{H}$ into the complex numbers such that:

**Mathematics**

1) $(u,u) = 0$ iff $u = 0$
2) $(u,v) = (v,u)^*$
3) $(u,v+w) = (u,v) + (u,w)$
4) $(u,\lambda v) = \lambda (u,v)$
4') $(\lambda u,v) = \lambda^* (u,v)$

**Quantum Mechanics**

1) $\langle u | u \rangle = 0$ iff $u = 0$
2) $\langle u | v \rangle = \langle v | u \rangle^*$
3) $\langle u | v+w \rangle = \langle u | v \rangle + \langle u | w \rangle$
4) $\langle u | \lambda v \rangle = \lambda \langle u | v \rangle$
4') $\langle \lambda u | v \rangle = \lambda^* \langle u | v \rangle$

* – denotes complex conjugation
The wavefunctions (previously denoted $|\Psi\rangle$) and quantum bits or qubits that arise from quantum mechanics live in a Hilbert space $\mathcal{H}$ (which may be finite and in the specific case of a single qubit: 2-dimensional). A Hilbert space $\mathcal{H}$ is a vector space over the complex numbers with a complex valued inner product. A complex valued inner product is a map: $(-,-): \mathcal{H} \times \mathcal{H}^\text{fi} \to \mathbb{C}$ from $\mathcal{H} \times \mathcal{H}$ into the complex numbers such that:

1) $(u,u) = 0$ iff $u = 0$
2) $(u,v) = (v,u)^*$
3) $(u,v+w) = (u,v) + (u,w)$
4) $(u,\lambda v) = \lambda (u,v)$
4') $(\lambda u,v) = \lambda^* (u,v)$

* denotes complex conjugate
Math. Defn for Dirac Notation

The elements or state vectors of the Hilbert Space \( \mathcal{H} \) are called ket vectors and are denoted as \( |label_1\rangle \). The elements of the dual space \( \mathcal{H}^* \) are called bra vectors and are denoted \( \langle label_2 | \). More formally, the linear functional \( \langle label_2 | \) is a linear operation which associates a complex number with every ket \( |label_1\rangle \). This set of linear functionals defined on the kets \( |label_1\rangle \) constitutes a vector space called the dual space of \( \mathcal{H} \) and is denoted \( \mathcal{H}^* \).

The complex inner product, denoted by a bra-c-ket is

\[
\langle label_1 | label_2 \rangle = (|label_1\rangle, |label_2\rangle)
\]

There is a isomorphic mapping on \( \mathcal{H} \) (assuming it is finite dimensional) that maps it into \( \mathcal{H}^* \) defined by \( |label\rangle \mapsto (|label\rangle, -) \) and denoted by the bra \( \langle label | \).

All linear properties shown on the previous slide apply!
Qubits, Basis Sets, and Superposition

In most of the following we will concern ourselves with quantum bits or “qubits” that like classical bits have only two elementary orthonormal basis states. Thus even though quantum systems may have many states we will focus on the two lowest states. These states we will denote hereafter as the abstract basis vectors $|0\rangle$ and $|1\rangle$, where

$$\langle 0|0 \rangle = \langle 1|1 \rangle = 1 \quad \text{and} \quad \langle 0|1 \rangle = \langle 1|0 \rangle = 0$$

Although the original Hilbert Space $H$ may have been d-dimensional, only the 2-dimensional $H$ spanned by $\{ |0\rangle, |1\rangle \}$ are relevant for quantum information. An arbitrary state $|\Psi\rangle$ can thus be represented as a superposition of $|0\rangle$ and $|1\rangle$

$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad \{\alpha, \beta\} \in \mathbb{C} \quad \text{where} \quad \alpha^* \alpha + \beta^* \beta = 1$$

since

$$\langle \Psi |\Psi \rangle = 1 = (\alpha^* \langle 0| + \beta^* \langle 1|)(\alpha |0\rangle + \beta |1\rangle)$$

Consequently, the resulting single qubit $H$ is equivalent to the vector space $\mathbb{C}^2$. 
The state $|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle$, which is an arbitrary superposition of the qubit basis sets $|0\rangle$ and $|1\rangle$, can be represented using the Bloch sphere. Assuming $|\Psi\rangle$ is normalized, then it is obvious that

$$\langle \Psi | \hat{O} | \Psi \rangle = \langle \Phi | \hat{O} | \Phi \rangle$$

for an arbitrary operator $\hat{O}$, if $|\Phi\rangle = e^{ix} |\Psi\rangle$ — i.e., $|\Psi\rangle$ and $|\Phi\rangle$ represent the same state since they differ at most by a constant.

Thus

$$|\Psi\rangle = a |0\rangle + \beta |1\rangle \quad a \in \mathbb{C} \quad \text{and} \quad \beta' \in \mathbb{C} \quad \text{where} \quad a^2 + \beta'^* \beta' = 1$$

$$|\Psi\rangle = a |0\rangle + e^{i\varphi} b |1\rangle \quad \{a,b\} \in \mathbb{C} \quad \text{where} \quad a^2 + b^2 = 1$$

which leads to:

$$|\Psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle$$

From E. Knill
Physical Representation of a Qubit

A one-electron atom:

- lower energy state: \( |0\rangle \)
- higher energy state: \( |1\rangle \)

An atom can be \( |0\rangle \) or it can be \( |1\rangle \) but it can also be \( \frac{|0\rangle + |1\rangle}{\sqrt{2}} \)

\( i.e. \) -- quantum superpositions are possible

\[ |\Psi\rangle = \alpha |0\rangle + \beta |1\rangle \]
Matrix Representations of Qubits

\[ |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \]

\[ |\Psi\rangle = \alpha |0\rangle + \beta |1\rangle = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \]

The “bra” \( \langle \text{label} | \) appropriate to the “ket” \( | \text{label}\rangle \) is given by the complex conjugate – transpose. Thus,

\[ \langle 0 | = \begin{pmatrix} 1 & 0 \end{pmatrix} \text{ and } \langle 1 | = \begin{pmatrix} 0 & 1 \end{pmatrix} \]

\[ \langle \Psi | = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} \]

As a result it is trivial to show:

\[ \langle 0 | 0 \rangle = \langle 1 | 1 \rangle = 1 \text{ and } \langle 1 | 0 \rangle = 0 ; \]

\[ \langle \Psi | \Psi \rangle = \alpha^* \alpha + \beta^* \beta = |\alpha|^2 + |\beta|^2 \]
A projection operator for the subspace spanned by the ket $|\text{label}\rangle$ is given by:

$$P_{\text{label}} = |\text{label}\rangle\langle\text{label}|$$

$$\hat{P}_0 = |0\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\hat{P}_1 = |1\rangle\langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\hat{P}_\Psi = |\Psi\rangle\langle\Psi| = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} = \begin{pmatrix} \alpha\alpha^* & \alpha\beta^* \\ \beta\alpha^* & \beta\beta^* \end{pmatrix}$$

Thus:

$$\hat{P}_0 |\Psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ 0 \end{pmatrix} = \alpha |0\rangle$$

$$\hat{P}_0 |\Psi\rangle = |0\rangle\langle 0| |\Psi\rangle = |0\rangle\langle 0| \{\alpha |0\rangle + \beta |1\rangle\} = \alpha |0\rangle$$

$$\langle\Psi|\hat{P}_0 |\Psi\rangle = \langle\Psi|0\rangle\langle 0| |\Psi\rangle = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha^*\alpha = |\alpha|^2$$
Quantum Measurement

Quantum measurement is just a projection onto the measurement basis. Thus if we measure the state $|\Psi\rangle$ in the basis $\{|0\rangle, |1\rangle\}$, then the probability of getting $|0\rangle$ is:

$$\langle \Psi | \hat{P}_0 | \Psi \rangle = \langle \Psi | 0 \rangle \langle 0 | \Psi \rangle = |\alpha|^2$$

Assuming I obtained the measurement $|0\rangle$, then the new state of the system is:

$$\frac{\hat{P}_0 | \Psi \rangle}{\sqrt{\langle \Psi | \hat{P}_0 | \Psi \rangle}} = \frac{|0\rangle \langle 0 | \Psi \rangle}{\sqrt{\langle \Psi | 0 \rangle \langle 0 | \Psi \rangle}} = |0\rangle$$

Basically the term in the denominator, renormalizes the state. Repeating the measurement on this system will return the same result!
Quantum Observables for Experts

- Quantum observables are represented by linear Hermitian operators – *i.e.* \( \hat{A} = \hat{A}^H = \hat{A}^\dagger = \hat{A}^{T*} \)

- The eigenvalues \( a_j \) of an observable \( A \) are real
  \[ \hat{A} \left| \Psi_{a_j} \right\rangle = a_j \left| \Psi_{a_j} \right\rangle \quad \text{or} \quad \hat{A} \left| a_j \right\rangle = a_j \left| a_j \right\rangle \]

- For Hermitian operators one can write:
  \[ \hat{A} = \sum_{j=0}^{n-1} a_j \left| a_j \right\rangle \langle a_j \right| = \sum_{j=0}^{n-1} a_j P_{a_j} \]

- Moreover the projection operators are mutually orthogonal and complete
  \[ \sum_{j=0}^{n-1} P_{a_j} = \hat{I} = 1 \]

- And finally an arbitrary state \( \left| \Psi \right\rangle \) in \( H \) can be decomposed as
  \[ \left| \Psi \right\rangle = \sum_{j=0}^{n-1} P_{a_j} \left| \Psi \right\rangle = \sum_{j=0}^{n-1} a_j \left| a_j \right\rangle \langle a_j \left| \Psi \right\rangle \]
Quantum Interference

- Waves coming through two slits interfere
Quantum Particle Interference

\[ I(x) \neq I_1(x) + I_2(x) \]

Electron Gun

Double Slit

\[ I(x) \propto |E(x)|^2 = |E_1(x) + E_2(x)|^2 \]

where \( E(x) = E_1(x) + E_2(x) \)
Quantum and the Atom

- Discrete Energy Levels
- Alternative Representation
- Transition
- Spectrum

- Photons as particles
- Atoms as particles/waves
- Wave-Particle Duality (deBroglie waves)
- Wave both here and there
Superposition and Measurement

- Quantum Superposition

\[ |\Psi\rangle = (x|0\rangle + y|1\rangle) \]

- Probability of being in “|0⟩”

\[ |\langle 0 | \Psi \rangle|^2 = \langle \Psi | 0 \rangle \langle 0 | \Psi \rangle = x^2 * \]

- Example a π/2 Pulse

\[ |\Psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \]

- Quantum Measurement

The act of observing or projecting a system into one of its natural states. Thus the system ends up in a new state \[ |\Psi_n\rangle \]

Measurement in |0⟩: \[ |\langle 0 | \Psi \rangle|^2 = \langle \Psi | 0 \rangle \langle 0 | \Psi \rangle \] with probability: \[ |x|^2 \]
From 1-Qubit to 2-Qubits

Single Qubit: \[ |\Psi_1\rangle = (\alpha_1 |0\rangle + \beta_1 |1\rangle) \]

2-Qubit State: \[ |\Psi_1\rangle \otimes |\Psi_2\rangle = (\alpha_1 |0\rangle + \beta_1 |1\rangle) \otimes (\alpha_2 |0\rangle + \beta_2 |1\rangle) \]

basis set for particle 1 basis set for particle 2

\[ = \alpha_1 \alpha_2 |00\rangle + \alpha_1 \beta_2 |01\rangle + \beta_1 \alpha_2 |10\rangle + \beta_1 \beta_2 |11\rangle \]

denotes a 2-qubit basis state – i.e. \[ |00\rangle \]

\[ = \alpha_1 \alpha_2 |0\rangle_2 + \alpha_1 \beta_2 |1\rangle_2 + \beta_1 \alpha_2 |2\rangle_2 + \beta_1 \beta_2 |3\rangle_2 \]

Product states span a 2-dimensional Hilbert space

2-Qubit product states have the property that the product of the coefficients of the \[ |00\rangle \] and \[ |11\rangle \] term equals the product of the \[ |01\rangle \] and \[ |10\rangle \] term!

Are there a different class of 2-qubit states?
**Quantum Entanglement**

2-Qubit Entangled State (unfactorizable):

\[ |\Psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle_1 |0\rangle_2 + |1\rangle_1 |1\rangle_2) = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \]

*not* a product state; can span a 4-dimensional Hilbert space

Entanglement creates a “shared fate” **Schrodinger’s Cat**

Another example of an unfactorizable 2-qubit state:

\[ |\Psi\rangle_2 = \alpha |00\rangle + \beta |01\rangle + \gamma |10\rangle + \delta |11\rangle \]

and \( \alpha\delta \neq \beta\gamma \)

Note -- however if \( \alpha\delta = -\beta\gamma \), then:

\[ |\Phi\rangle_2 = \alpha |00\rangle + \beta |01\rangle + \gamma |10\rangle - \delta |11\rangle \]

is factorizable!!

Entanglement is a unique *quantum* resource:

“... fundamental resource of nature, of comparable importance to energy, information, entropy, or any other fundamental resource.”

Nielsen & Chuang, Quantum Computation and Quantum Information
Tensor Products

Let $/_1$ and $/_2$ be two separate (possibly identical) quantum systems that have been independently prepared in states described by $|\Psi_1\rangle$ and $|\Psi_2\rangle$. Assuming these two quantum systems $/_1$ and $/_2$ have not interacted since their preparation, then the combined wavefunction for the quantum system can be represented as a tensor product $– i.e.$

$$|\Psi_{total}\rangle = |\Psi_1\rangle \otimes |\Psi_2\rangle$$

$$|\Psi_1\rangle \otimes |\Psi_2\rangle \in H_1 \otimes H_2$$

More formally, given $n$-quantum systems, $/_1,/_2, \ldots,/_n$, characterized by the Hilbert spaces, $H_1, H_2, \ldots, H_n$, respectively, then the multipartite quantum system has a Hilbert space $H$ given by:

$$H = \bigotimes_{j=1}^{n} H_j$$

NOTE!! – However, the general state $|\Psi\rangle$ of a quantum system cannot be represented as tensor product of individual component wavefunctions $|\Psi_j\rangle$ – i.e. generally $|\Psi\rangle \neq \bigotimes_{j=1}^{n} |\Psi_j\rangle$.
**Matrix Representations of Tensors**

2-Qubit Basis States:

\[
|0\rangle_2 = |00\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} ; \quad |1\rangle_2 = |01\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}
\]

\[
|2\rangle_2 = |10\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} ; \quad |3\rangle_2 = |11\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}
\]

A more general 2-Qubit Basis Product State:

\[
|\Psi\rangle_2 = |\Psi_1\rangle \otimes |0\rangle = \{\alpha |0\rangle + \beta |1\rangle\} \otimes |0\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha \\ 0 \\ \beta \\ 0 \end{pmatrix}
\]
Interesting $n$-particle Tensor States

The equal superposition of all possible $(2^n)$ $n$-qubit states is a tensor product – Proof:

$$|\Psi\rangle_n = \left\{ \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right\}^\otimes$$

$$= \left( \frac{1}{\sqrt{2}} \right)^n \{ |00\cdots00\rangle + |00\cdots01\rangle + |00\cdots10\rangle + \cdots + |11\cdots11\rangle \}$$

$$= \left( \frac{1}{2^{n/2}} \right)^n \{ |0\rangle_n + |1\rangle_n + |2\rangle_n + \cdots + |2^n - 1\rangle_n \}$$

Note – in general an $n$-qubit state is defined by $2^n$ complex coefficients and therefore is defined by $4^n - 2$ real numbers since the overall phase is arbitrary and the total wavefunction should be normalized.
A very good overall reference is *Quantum Computation and Quantum Information* by M. A. Nielsen and I. L. Chuang.

For a general introduction to Quantum Mechanics see *Quantum Mechanics* by C. Cohen-Tannoudji, B. Diu, and F. Laloë (especially Chapters 2-4).

For a mathematical view of Quantum Mechanics see *Linear Operators for Quantum Mechanics* by T. F. Jordan.

For more on Dirac Notation see *The Principles of Quantum Mechanics* by P. A. M. Dirac (especially Chapter 1).


IV. Classical Bits vs. Quantum Bits

- **Classical Bits**: two-state systems
  Classical bits: 0 (off) or 1 (on) (switch)

- **Quantum Bits** are also two-state (level) systems
  Note that almost all quantum systems have more than 2-states and thus a qubit is really using just 2-states of an $n$-state quantum system!

\[
\Psi = \alpha |\uparrow\rangle + \beta |\downarrow\rangle
\]

But: Quantum Superpositions are possible

\[
= \alpha |0\rangle + \beta |1\rangle
\]
Scaling of Quantum Information

- **Classically**, information stored in a bit register: a 3-bit register stores one number, from 0 – 7.  
  \[ \begin{array}{ccc} 0 & 1 & 0 \end{array} \]

  *e.g.*  
  \[ \begin{array}{ccc} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{array} \ldots \begin{array}{ccc} 1 & 1 & 1 \end{array} \]

- **Quantum mechanically**, a 3-qubit register can store all of these numbers in an arbitrary superposition:

  \[ \alpha |000\rangle + \beta |001\rangle + \chi |010\rangle + \delta |011\rangle + \epsilon |100\rangle + \gamma |101\rangle + \eta |110\rangle + \kappa |111\rangle \]

- **Result:**
  - Classical: one N-bit number
  - Quantum: \(2^N\) (all possible) N-bit numbers
Scaling of Quantum Information (2)

• Consequence of Quantum Scaling
  – Calculate all values of \( f(x) \) at once and in parallel
  – Quantum Computer will provide Massive Parallelism

• But wait …
  – When I “readout the result” I obtain only one value of \( f(x) \)
  – For the previous 3-qubit example each value of \( f(x) \) appears with probability 1/8

• Thus must measure some global property of \( f(x) \)
  – *e.g.* periodicity

Note!

300-qubit register has much more storage capacity than classically is in the whole universe
33-qubits has 1Gb of storage capacity
Is a quantum computer basically an analogue computer – (qubit coefficients are continuous)?

No!

• Why Not? – Analog Computer
  – Finite Resolution ⇒ must bin values
  – Scaling lost ⇒ equivalent to classical digital computer
    ⇒ classical Church-Turing hypothesis

• Quantum Computer
  – Add 1 qubit, double storage/memory capacity
  – Scaling is preserved ⇒ tensor product structure and entanglement
Einstein-Podolsky-Rosen Paradox

\[ |0_1\rangle|0_2\rangle + |1_1\rangle|1_2\rangle \]  

(1) Prepare 2-qubits in an entangled state

(2) Send qubit 1 with Alice to Paris and qubit 2 with Bob to Tokyo

before measurement, \( \textcircled{1} \) is both \(|0_1\rangle\) and \(|1_1\rangle\) (as is \( \textcircled{2} \) !)

But if you measure \( \textcircled{1} \) to be \(|0_1\rangle\), then \( \textcircled{2} \) is surely \(|0_2\rangle\)

And you know it immediately, even if \( \textcircled{2} \) is light years away
No Cloning Theorem

Assume there exists a unitary operator $\hat{U}_{\text{clone}}$ that copies an arbitrary unknown quantum states into a standard or “null” state. Then for two arbitrary states $|\Psi\rangle$ and $|\Phi\rangle$ such that:

$|\Psi\rangle \neq |\Phi\rangle$ and $\langle\Psi | \Phi \rangle \neq 0$

one can then write:

$\hat{U}_{\text{clone}} |\Psi\rangle |0\rangle = |\Psi\rangle |\Psi\rangle$

$\hat{U}_{\text{clone}} |\Phi\rangle |0\rangle = |\Phi\rangle |\Phi\rangle$

Taking the Hermitian conjugate of the lower equation and equation and collecting the left and right sides one obtains:

$\langle 0 | \langle \Phi | \hat{U}_{\text{clone}} ^\dagger \hat{U}_{\text{clone}} |\Psi\rangle |0\rangle = \langle \Phi | \langle \Phi | |\Psi\rangle |\Psi\rangle$

$\langle 0 | \langle \Phi | |\Psi\rangle |0\rangle = \langle \Phi | |\Psi\rangle ^2$

$1 = \langle \Phi | |\Psi\rangle$

This is a clear contradictions and thus $\hat{U}_{\text{clone}}$ must not exist!
Quantum Circuits

A timeline for a single qubit

A gate on a single qubit

A controlled unitary gate where the state of the control $|\chi\rangle$ determines whether $U$ is applied

A controlled-not gate where the control flips the target

A controlled-controlled unitary gate where iff the two control qubits have a component \(|11\rangle\) is the unitary applied to the $3^{rd}$

Note: Because of entanglement, one must be careful to interpret the circuit by linearly applying the appropriate set of gates on each of the individual components of the qubit bases functions $|0\rangle$ and $|1\rangle$ that span the $H$ space – i.e. use the linear properties of the vector space.
Standard Single Qubit Gates

- Hadamard
  \[ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \]
  - A very important & key 1-qubit gate

- Pauli-X
  \[ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \]
  - The basic 1-qubit bit-flip gate

- Pauli-Y
  \[ \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \]
  - A basic gate for a 1-qubit phase error

- Pauli-Z
  \[ \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \]

- Phase
  \[ \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \]

- π/8
  \[ \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \]

Notes:
- A very important & key 1-qubit gate
- The basic 1-qubit bit-flip gate
- A basic gate for a 1-qubit phase error
Common $n$-Qubit Gates

- Controlled-NOT

- Classical Bit

- Toffoli

- Swap

- Fredkin or controlled swap

- Measurement

- Controlled-Z or controlled “phase”
Example of CNOT Gate

Let:  \[ |\Psi\rangle_{12} = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \]

\[
\begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{pmatrix}
\begin{pmatrix}
\alpha \\
\beta \\
\gamma \\
\delta
\end{pmatrix} =
\begin{pmatrix}
\alpha \\
\beta \\
\gamma \\
\delta
\end{pmatrix}
\]

\[ \Rightarrow |\Psi\rangle_{12} = \alpha|00\rangle + \beta|01\rangle + \delta|10\rangle + \gamma|11\rangle \]

If \( \alpha = \gamma = \frac{1}{\sqrt{2}} \) and \( \beta = \delta = 0 \); then
\[ |\Psi\rangle_{12} = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \]

\[ \Rightarrow \text{CNOT} \quad |\Psi\rangle_{12} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \]

**1- & 2-Qubit Gates allow for all possible unitary operations**

\[ |\Psi_{initial}\rangle_{N\text{-bit}} \xrightarrow{Q} |\Psi_{final}\rangle_{N\text{-bit}} \]
No Cloning Theorem – Revisited

• Copying a Classical Bit

\[
\begin{align*}
\{c\} & \rightarrow \{c\} \\
\{t\} & \rightarrow \text{mod}(c+t,2)
\end{align*}
\]

• Attempt to Copy a Quantum Bit:

\[
\begin{align*}
|\varphi_1\rangle & \rightarrow "\varphi_1"? \\
|\varphi_2\rangle & \rightarrow "\text{mod}(\varphi_1 + \varphi_2,2)"
\end{align*}
\]

Then:

\[
|\varphi_1\varphi_2\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \neq \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) = \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle)
\]

entangled state

|Truth Table|
\[
\begin{align*}
\{c,t\} & \rightarrow \{c,\text{mod}(c+t,2)\} \\
\{00\} & \rightarrow \{00\} \\
\{01\} & \rightarrow \{01\} \\
\{10\} & \rightarrow \{11\} \\
\{11\} & \rightarrow \{10\}
\end{align*}
\]

|Let:|
\[
|\varphi_1\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \\
|\varphi_2\rangle = |0\rangle
\]
Applications of Quantum Information

• Quantum Communication - 100% physically secure
  – Quantum cryptographic key exchange – generation of a one-time classical key for secure communication
  – Quantum Teleportation – requires “entangled photons”

• Quantum Algorithms and Computing
  – Factorization of large composite numbers
  – Searching large databases
  – Potential solution of computationally intractable (NP) problems
  – Simulation of large-scale quantum systems

• Quantum Measurement – improved accuracy
  – Beats classical limit on Signal to Noise $\propto 1/N$ vs $\propto 1/\sqrt{N}$
  – Better Atomic Clocks
  – Metrology for Single Photon Sources and Detectors

**Note:** Quantum Computing requires larger register size and higher fidelity gates then either Quantum Communication or Quantum Measurement.
V. Quantum Communication

- **Quantum Key Distribution** – attenuated or single photon sources with known but arbitrary selected polarization and an authenticated classical channel

- **Quantum Teleportation** – *i.e.* “sending” of an unknown quantum state – **requires** shared Bell’s (entangled) states and an authenticated classical channel

- **Dense Coding** – **requires** shared Bell’s states

- **Quantum Communication:**
  - with attenuated sources is 100% physically secure and has been demonstrated over kilometer distances
  - in fibers over distances larger than ~100 km will require quantum repeaters
  - ~ 10 qubit quantum processors can serve as quantum repeaters
Eve freely copies classical bits – encryption may delay reading of message.
Quantum Communication

Eve can only obtain key bits by destroying them (no-cloning theorem). Eve presence is detected.
Basis for BB84

Two non-orthogonal Alphabets

**Horizontal/Vertical**

\[
\begin{align*}
|0_H\rangle & \\
|1_H\rangle & \\
\end{align*}
\]

**Diagonal**

\[
\begin{align*}
|0_D\rangle & \\
|1_D\rangle & \\
\end{align*}
\]

Relation between Basis Sets:

\[
\langle \Psi_D | \Psi_H \rangle = \begin{pmatrix}
1 \\
\sqrt{2} \\
-1 \\
\sqrt{2}
\end{pmatrix}
\begin{pmatrix}
1 \\
\sqrt{2} \\
1 \\
\sqrt{2}
\end{pmatrix}
\]

If you measure either \(|0_H\rangle\) or \(|1_H\rangle\) in the diagonal basis you have a 50% probability of obtaining \(|0_D\rangle\) or \(|1_D\rangle\). Similarly if you measure \(|0_D\rangle\) or \(|1_D\rangle\) in the horizontal basis. Easily obtained using simple trigonometry.
**BB84 Protocol Schematic**

- Alice's single photon source
- Alice's polarization selector
- Two Basis sets (alphabets)
- quantum channel
- Bob's polarization analyzers
- Bob's result
- Same basis?
- Transmitted key

**Alice's bit value**: 1 0 0 0 1 1 1
**Alice's polarization**: \01/ \01/ \01/ \01/ \01/ \01/ \01/ 
**Bob's polarization basis**: × × + × + + × × + + × × + + 
**Bob's result**: 1 1 0 0 1 1
**Same basis?**: Y N N Y N Y
**Transmitted key**: 1 0 1 56
• **STEP 1: Transmission - *quantum channel***
  – Alice selects random key and transmits each bit using random basis
  – Bob measures each bit in random basis
  – Bob now has key, but only some are right

• **STEP 2: Reconciliation - *classical channel***
  – Bob tells Alice which *bases* he used (but not the data)
  – Alice tells Bob which bases match (the bits measured in the same bases should match – assuming no errors)
BB84 Protocol (2)

• Only bits transmitted and received using same basis are used as key

• STEP 3: Detecting Eve - classical channel
  – Alice & Bob compare initial bits of key
  – If key does not match, then it has been compromised
  – If error rate > 25%, must assume Eve is present
  – In practice other sources of error must be accounted for. Error correction and privacy amplification can be applied for error rates < 25%.
Bell States and Teleportation

- Making Bell States

\[
\begin{align*}
|00\rangle & \quad \mapsto \quad \begin{pmatrix} |00\rangle + |11\rangle \big/ \sqrt{2} \\ |01\rangle + |10\rangle \big/ \sqrt{2} \\ |00\rangle - |11\rangle \big/ \sqrt{2} \\ |01\rangle - |10\rangle \big/ \sqrt{2} \end{pmatrix} \\
|\beta_{00}\rangle & \quad \equiv \quad \begin{pmatrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{pmatrix}
\end{align*}
\]

- Teleportation

\[
\begin{align*}
|\Psi\rangle & \quad \mapsto \quad \begin{pmatrix} |00\rangle \big/ \sqrt{2} \\ |10\rangle \big/ \sqrt{2} \end{pmatrix} \\
|\beta_{00}\rangle & \quad \equiv \quad \begin{pmatrix} |\beta_{00}\rangle \\ |\beta_{10}\rangle \end{pmatrix}
\end{align*}
\]
Analysis of Teleportation Circuit

\[ |\Psi\rangle \]

\[ |\beta_{00}\rangle \]

\[ |\psi_0\rangle, |\psi_1\rangle, |\psi_2\rangle \]

\[ |\Psi_0\rangle = |\Psi\rangle \otimes |\beta_{00}\rangle = \frac{1}{\sqrt{2}} \left[ \alpha |0\rangle \otimes (|00\rangle + |11\rangle) + \beta |1\rangle \otimes (|00\rangle + |11\rangle) \right] \]

\[ |\Psi_1\rangle = \frac{1}{\sqrt{2}} \left[ \alpha |0\rangle \otimes (|00\rangle + |11\rangle) + \beta |1\rangle \otimes (|10\rangle + |01\rangle) \right] \]

\[ |\Psi_2\rangle = \frac{1}{2} \left[ |00\rangle \otimes (\alpha |0\rangle + \beta |1\rangle) + |01\rangle \otimes (\alpha |1\rangle + \beta |0\rangle) + |10\rangle \otimes (\alpha |0\rangle - \beta |1\rangle) + |11\rangle \otimes (\alpha |1\rangle - \beta |0\rangle) \right] \]

60
Status of Quantum Communications

• State of the Art
  – Free Space
    – 10 km both day and night: LANL
    – 30 km night: Kurtseifer, Rarity
  – Fiber over 65km
    – LANL, Telcordia
    – U. Geneva: Gisin
    – MagiQ

• Wish List
  – Single Photon Sources: Numerous Demonstrations
  – High Efficiency Single Photon Detectors
  – Quantum Repeaters
NIST Testbed Structure

1.25 GHz High-speed QKD
Quantum Communication Test-Bed

What is special about the NIST system?

- **Dual Classical & Quantum Channels running at 1.25 GHz**
- **Network – Internet interfaced (Also BBN)**
  - Security Protocols – SSL, Authentication
- **Quantum Link**
  - Attenuated VCSEL transmitters (initially)
  - 850 nm free space optics
  - Si avalanche detectors
- **Two classical links near 1550 nm**
  - 8B/10B encoded path for timing/framing
  - Dedicated gigabit ethernet channel
    - Sifting, Error correction, and Reconciliation
    - Privacy amplification

Joshua Bienfang, Bob Carpenter, Alex Gross, Ed Hagley, Barry Hershman, Richang Lu, Alan Mink, Tassos Nakassis, Xiao Tang, Jesse Wen, David Su, Charles Clark, Carl Williams
High-Speed Free-Space QKD

- Spectral, Spatial filter to $\sim 10^6$ solar photons/sec into Rx
  - $(0.1 \text{ nm}, 300 \text{ cm}^2, 220 \mu\text{rad})$

- Gating:

  8B/10B encoding/clock recovery

- No heralding pulse: all time bins are filled
- A 1 ns gate is equivalent to 1 GHz pulse rate
  - Gate shortens with increased pulse rate
  - Limited by detector jitter and recovery time
VI. Quantum Computing

- A Uniform Superpositions of all input states is easy:

\[ |\Psi\rangle_n = \left\{ \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right\}^\otimes n \]

\[ = \left( \frac{1}{\sqrt{2}} \right)^n \{ |00\cdots00\rangle + |00\cdots01\rangle + |00\cdots10\rangle + \cdots + |11\cdots11\rangle \} \]

- Using \( n \)-additional qubits calculate the function \( f \) on \( |\Psi\rangle_n \)

\[ |\Psi_n\rangle \quad \text{The result is entanglement between } |\Psi\rangle_n \text{ and its function} \]

\[ |\Psi_f (\Psi)\rangle_n = \left( \frac{1}{2^n/2} \right) \{ |0\rangle_n \left| f \left( |0\rangle_n \right) \right\rangle + |1\rangle_n \left| f \left( |1\rangle_n \right) \right\rangle + \cdots + 2^n - 1 \rangle_n \left| f \left( 2^n - 1 \rangle_n \right) \right\rangle \} \]
Classical vs Quantum Computation

Classical Computation

- Initialize state: “0”
- Logic:
  - *not*  
    - 0 → 1
    - 1 → 0
  - *and*  
    - 00 → 0
    - 01 → 0
    - 10 → 0
    - 11 → 1
- Output result
- Logic errors:
  - Error correction possible

Quantum Computation

- Initialize state: \( \Psi_{in} = |000\cdots0\rangle \)
- Logic:
  - 1-qubit
    - |0\rangle → |1\rangle
    - \(|0\rangle \rightarrow (|0\rangle + |1\rangle)/2^{1/2} \)
  - 2-qubit
    - controlled-not
      - 00 → 00
      - 01 → 01
      - 10 → 11
      - 11 → 10
- Final state measurement
  - Measure qubits
    - \( \Psi_f = |ijk\cdots l\rangle \)
  - Coherence:
    - \( \tau_{coherence}/\tau_{logic} \approx 10^4 \)

Q. Computation allows non-classical computation
Universal Quantum Logic

**All quantum computations and all unitary operators may be efficiently constructed from 1- and 2- qubit logic gates**

**Single Qubit Operations/Gates**

**Arbitrary 1-qubit rotations:**

\[ |0\rangle \rightarrow \alpha |0\rangle + \beta |1\rangle \]

\[ |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} ; \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} ; \quad \begin{pmatrix} \alpha & -\beta^* \\ \beta & \alpha^* \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \]

**Note:** Although the standard paradigm for quantum computations relies on the ability to do arbitrary 1- qubit gates and almost any 2- qubit gates, alternatives exist
Most common 2-Qubit Gate: CNOT Gate

\[
\begin{align*}
|c,t\rangle & = (1\ 0\ 0\ 0) \\
|00\rangle & = (1\ 0\ 0\ 0) \\
|01\rangle & = (0\ 1\ 0\ 0) \\
|10\rangle & = (0\ 0\ 0\ 1) \\
|11\rangle & = (0\ 0\ 1\ 0)
\end{align*}
\]

This gate is similar to addition modular 2 of classical gates but one should recall that this gate works on arbitrary superpositions.
Bell States and Teleportation

• Making Bell States

\[ \begin{bmatrix}
|00\rangle \\
|01\rangle \\
|10\rangle \\
|11\rangle
\end{bmatrix} \xrightarrow{H, \beta_{xy}} \begin{bmatrix}
( |00\rangle + |11\rangle)/\sqrt{2} \\
( |01\rangle + |10\rangle)/\sqrt{2} \\
( |00\rangle - |11\rangle)/\sqrt{2} \\
( |01\rangle - |10\rangle)/\sqrt{2}
\end{bmatrix} \equiv \begin{bmatrix}
|\beta_{00}\rangle \\
|\beta_{01}\rangle \\
|\beta_{10}\rangle \\
|\beta_{11}\rangle
\end{bmatrix} \]

• Teleportation

\[ |\Psi\rangle \xrightarrow{H} |\Psi\rangle \]

\[ |\beta_{00}\rangle \xrightarrow{M_1} \]

\[ |\Psi\rangle \xrightarrow{M_2} X^{M_2} \xrightarrow{Z^{M_1}} |\Psi\rangle \]
Teleportation without Measurement

\[ |\Psi\rangle \]

\[ |\beta_{00}\rangle \{ \]

\[ \uparrow \uparrow \uparrow \uparrow \]

\[ H \]

\[ X \]

\[ Z \]

\[ |\Psi\rangle \]

\[ |\Psi\rangle = |\Psi\rangle \otimes |\beta_{00}\rangle = \frac{1}{\sqrt{2}} \left[ \alpha |0\rangle \otimes (|00\rangle + |11\rangle) + \beta |1\rangle \otimes (|00\rangle + |11\rangle) \right] \]

\[ |\Psi_1\rangle = \frac{1}{\sqrt{2}} \left[ \alpha |0\rangle \otimes (|00\rangle + |11\rangle) + \beta |1\rangle \otimes (|10\rangle + |01\rangle) \right] \]

\[ |\Psi_2\rangle = \frac{1}{2} \left[ |00\rangle \otimes (\alpha |0\rangle + \beta |1\rangle) + |01\rangle \otimes (\alpha |1\rangle + \beta |0\rangle) + |10\rangle \otimes (\alpha |0\rangle - \beta |1\rangle) + |11\rangle \otimes (\alpha |1\rangle - \beta |0\rangle) \right] \]

\[ |\Psi_3\rangle = \frac{1}{2} \left[ (|00\rangle + |01\rangle) \otimes (\alpha |0\rangle + \beta |1\rangle) + (|10\rangle + |11\rangle) \otimes (\alpha |0\rangle - \beta |1\rangle) \right] \]

\[ |\Psi_4\rangle = \frac{1}{2} \left[ (|00\rangle + |01\rangle + |10\rangle + |11\rangle) \otimes (\alpha |0\rangle + \beta |1\rangle) \right] \]
Quantum Error Correction

e.g. -- Redundant Encoding $|0\rangle_L = |000\rangle$ and $|1\rangle_L = |111\rangle$

$|\Psi\rangle_L = \alpha|000\rangle + \beta|111\rangle$

Measure Error Syndrome

extract error information (measure *parity*)
preserve original quantum information

Quantum Computing appears impossible without Quantum Error Correction (Shor, Steane,...)

opening bid:

$10^{-2}$ to $10^{-4}$ decoherence depends on errors, could improve
Basis of Shor’s Algorithm

- **N** – number to be factored
- select a number **x** such that \( \gcd(x, N) = 1 \) (coprime)
- find **r** such that \( x^r = 1 \pmod{N} \)
- **Example:** \( N = 15, x = 13 \)

\[
\begin{align*}
x^1 \pmod{15} &= 13 \\
x^2 \pmod{15} &= 4 \\
x^3 \pmod{15} &= 7 \\
x^4 \pmod{15} &= 1 \\
x^5 \pmod{15} &= 13 \\
x^6 \pmod{15} &= 4
\end{align*}
\]

\( r = 4 \) and \( \therefore x^r - 1 = 0 \) or for **r** even

\[
(x^{r/2} - 1)(x^{r/2} + 1) = 0 \pmod{N} = kN
\]

factors are \( (x^{r/2} \pm 1) \pmod{N} \)

- **e.g.** \( x = 4 \)

\[
\begin{align*}
x^1 \pmod{15} &= 4 \\
x^2 \pmod{15} &= 1
\end{align*}
\]

- **e.g.** \( x = 7 \)

\[
\begin{align*}
x^1 \pmod{15} &= 7 \\
x^2 \pmod{15} &= 4 \\
x^3 \pmod{15} &= 13 \\
x^4 \pmod{15} &= 1
\end{align*}
\]
Shor’s Algorithm

• Select N such that \( N = p \cdot q \)
• Find x such that \( \gcd(x,N) = 1 \) (coprime)
• Run Shor’s Algorithm

\[
|\Psi\rangle = |000\cdots\rangle
\]

\[
|\Psi\rangle = |000\cdots\rangle
\]

\[
f(x) = a^x \mod(N)
\]

\[
Q-FFT
\]

• Measure first register and obtain an approximation to r
• factors are \((x^{r/2} \pm 1) \mod(N)\)
Quantum Information’s Impact

• **Revolutionary**
  – Builds the physical foundation for information theory
  – Teaches us to examine the information content in real systems
  – Help us to develop a language to move quantum mechanics from a scientific to an engineering field

• **Quantum Limited Measurement will become available**

• **20th Century we used the particle/wave aspects of Quantum Mechanics:** Televisions, CRT’s, NMR …

• **21st Century we will use the coherence, entanglement, and tensor structure of quantum systems to build new, as yet unimagined, types of devices**

---

*Let me speculate: Quantum engineering will come and will allow us to extend the Moore’s Law paradigm based not on making things smaller but making them more powerful by using the laws of quantum mechanics.*
VIII. Conclusions

What is Quantum Information?

A radical departure in information technology, more fundamentally different from current IT than the digital computer is from the abacus.

A convergence of two of the 20th Century’s great revolutions

Quantum Mechanics
(i.e. atoms, photons, molecules)
“Matter”

Information
(i.e. books, data, pictures)
More abstract
Not necessarily material
Quantum Information Timeline

- **The known**
  - Quantum Communication
  - Quantum Measurement

- **The expected**
  - Quantum Computation
  - Quantum Engineered Photocells?
  - Quantum Widgets
  - Quantum Sensors?

- **The unlikely – impossible?**
  - Quantum Games & Toys
  - The as yet unimagined!!

Time (years):
0  5  10  ~15  20?  25??

Difficulty/Complexity
Quantum Mechanics at its simplest level reduces to solving a differential equation that determines the time evolution of quantum system. This equation includes the Hamiltonian $H$ which describes a systems kinetic and potential energies. The solution of this equation is a wavefunction $\Psi(r,t)$ which can be more briefly written as the “ket” $|\Psi(t)\rangle$. The wavefunction along with $H, fully describes the system.

This mathematical view of quantum mechanics has been confirmed experimentally – an untold number of times.

Note a “ket” is nothing but a vector. The same is true of a “bra” $\langle \Psi(t) |$. 

The next few pages provides a “physics” and “mathematics” view of quantum mechanics. I will not do justice to either group. The key point is that bra’s and ket’s are vectors.