



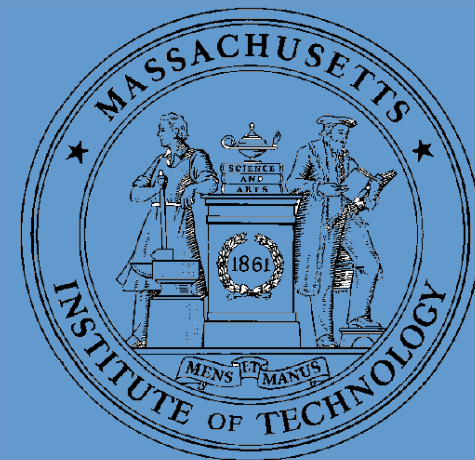
July 2, 2003

# Quantum Computation and Quantum information Theory

Patna Science College (January 17, 2004)

Saikat Guha

Research Laboratory of Electronics, MIT  
Cambridge, MA 02139  
USA





- **Principal Investigators:**
  - **Jeffrey H. Shapiro (Director, RLE), MIT**
  - **Franco N.C. Wong, MIT**
  - **Prem Kumar, NU**
  - **Selim Shahriar, NU**
  - **Horace Yuen, NU**

# Outline of the Talk

- Introduction
  - Physics and Information
  - Quantum Information: The 'Qubit'
  - New and Interesting Things one can do with Quantum Information
- Quantum Computing
  - Quantum Mechanics: Some Basics
    - Measurement, Entanglement, Density Operator, Quantum Logic Gates
  - Computing using Quantum Mechanics: Quantum Parallelism
  - Efficient Quantum Algorithms
    - Prime Factorization - Shor's Algorithm (Brief Discussion)
    - Quantum Search Algorithm (Brief Discussion)
  - Entanglement as a resource: 'Qubit Teleportation'

- Quantum Communication and Information Theory
  - Classical Information – Shannon Theory
    - Source Coding: Data Compression
    - Channel Capacity
    - Channel Coding: Error Correction
  - Quantum Channels – Quantum Information Theory
    - Information Capacity of a Quantum Channel
  - Free Space Quantum Optical Communication
    - Encoding Classical Information in the Optical Field and Optical Detection
    - Capacity of the Free Space Channel: Recent Advances
    - Ongoing Research in the Field
- MIT-NU Long Distance Teleportation Architecture
  - Challenges in implementation
  - Future Direction of Research

## ■ Physics and Information

- Information – something encoded in the state of a physical system.
- Computation – something that can be carried out on an actual physically realizable device.
- Landauer's Principle (1961) – erasure of information is necessarily 'dissipative'.  $W_{\text{one-bit}} = T\Delta S = kT \ln 2$
- Irreversible vs. Reversible Computation
  - **NAND:**  $(a, b) \rightarrow \sim(a.b)$
  - **TOFFOLI:**  $(a, b, c) \rightarrow (a, b, c+(a.b))$
- One 'BIT' of information: Szilard (1929)
- Foundation of Classical Information Theory: Claude Shannon (1948)

## ■ Quantum Information

- The universe is fundamentally quantum mechanical
- QUBIT:  $\alpha|0\rangle + \beta|1\rangle$ ;  $|\alpha|^2 + |\beta|^2 = 1$
- Tradeoff between acquiring information and creating a disturbance

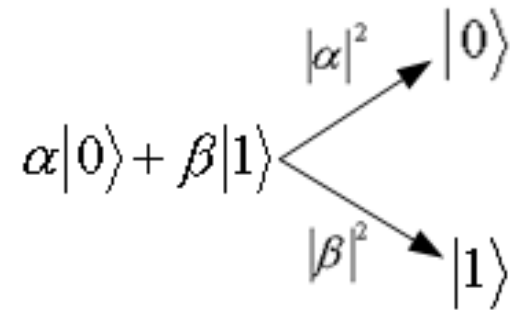
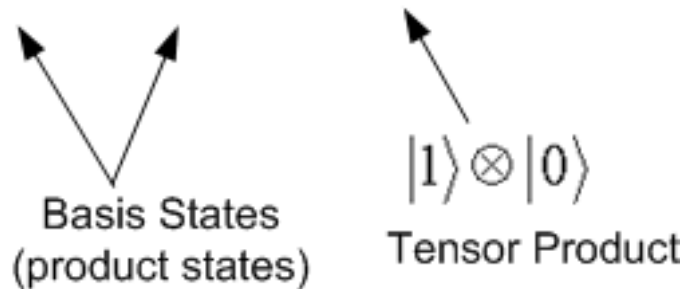
- Why Quantum ?
  - Any classical computation possible using quantum computing.
  - Solves classically intractable problems, eg. factoring.
  - Extremely high data rates of classical communication achievable over quantum channels.
  - Much better cryptosystems.
  - Teleportation!

# Quantum Computing

- Quantum Mechanics: Some Basics

- Measurement on a single QUBIT
- Multiple qubits

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$



- Entangled state  $\frac{1}{\sqrt{2}}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$

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

Product State

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Entangled State  
"Bell State"

- **Mixed States (Density Operator)**

$$\rho = |0\rangle\langle 0| \quad \left| \quad \rho = \sum_i w_i |\psi_i\rangle\langle \psi_i|$$

Pure State  $|0\rangle$                       Mixed State

$$\rho = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{4}|10\rangle\langle 10| + \frac{1}{4}|01\rangle\langle 01|$$

An Example of a 2-QUBIT mixed state

- **Quantum Unitary Evolution**

- Unitary :  $UU^\dagger = I$
- Unitarity  $\rightarrow$  Probability Conservation

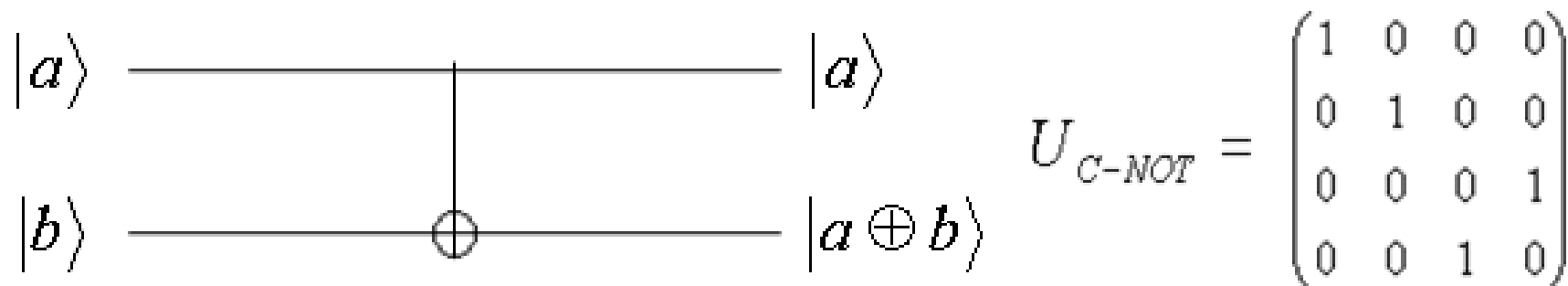
$$|\psi\rangle \longrightarrow U|\psi\rangle$$
$$\rho \longrightarrow U\rho U^\dagger$$

# Quantum Computing

- Quantum Logic Gates (Reversible Evolution)

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Examples of Single Qubit Operations (Gates)



C-NOT Gate : A 2-Qubit Operation

# Quantum Computing

$|x\rangle \rightarrow$  N - Qubit register

$$U_f : |x\rangle|0\rangle \rightarrow |x\rangle|f(x)\rangle$$

- Essence of Quantum Computing:

‘Massive Parallelism’

Choose the input register to be in the state:

$$\left[ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \right]^N = \frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} |x\rangle$$

By computing  $f(x)$  only once, we can generate the state:

$$\frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} |x\rangle|f(x)\rangle$$

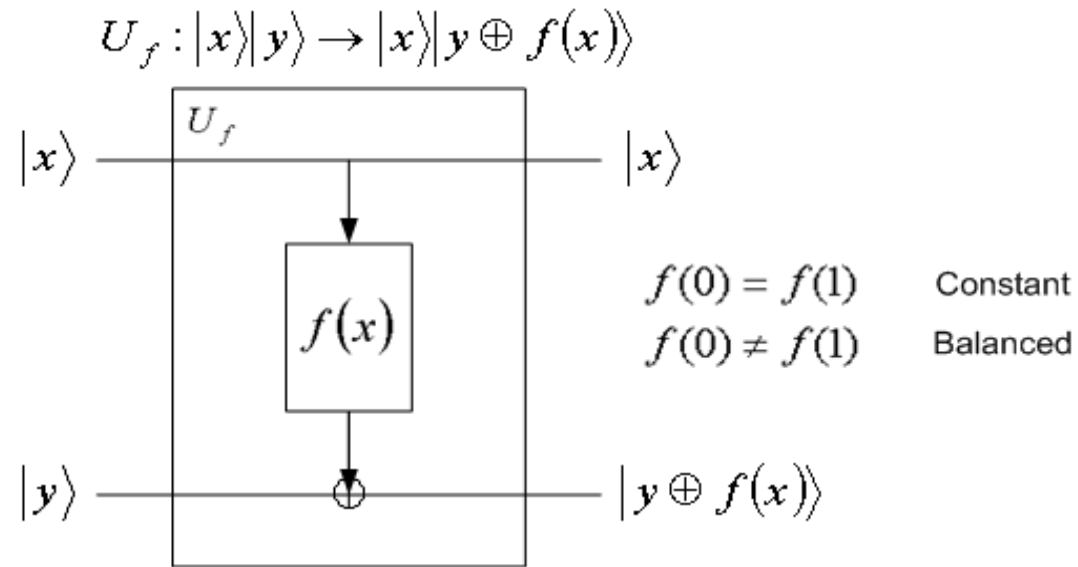
Caution !! don't measure right away!

Try something more clever ...

# Quantum Computing

- Computing using Quantum Mechanics:

A simple Example of “Quantum Parallelism”



Classically:

TWO queries of the black-box needed.

$$U_f : |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow |x\rangle \frac{1}{\sqrt{2}}(|f(x)\rangle - |1 \oplus f(x)\rangle)$$

$$= |x\rangle (-1)^{f(x)} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Quantum Mechanically:

ONE query of the black-box needed.

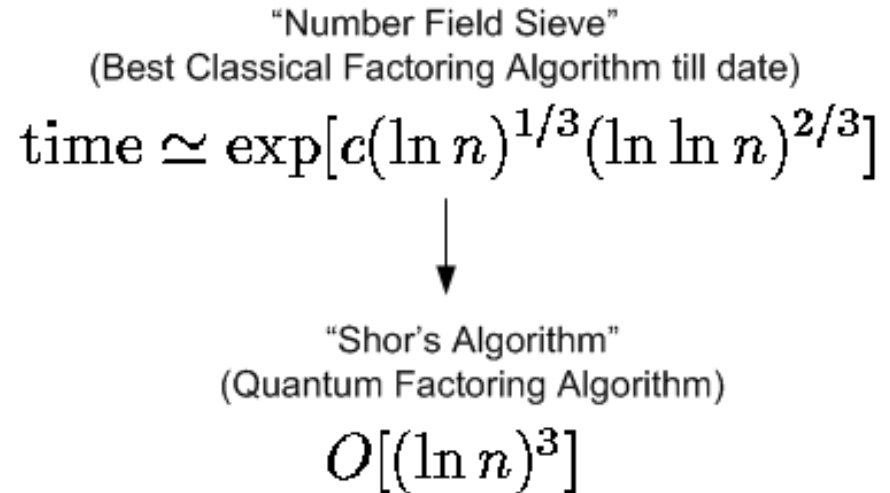
$$U_f : \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow$$

$$\frac{1}{\sqrt{2}} [(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle] \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

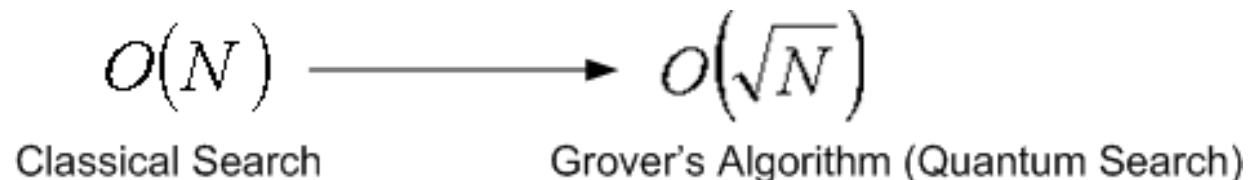
Measure in the basis:  $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$

# Quantum Computing

- Efficient Quantum Algorithms
  - Shor's Algorithm  
(Prime Factorization of a number  $n$ )



- Grover's Algorithm  
(Searching a random database of size  $N$ )



## ■ Qubit Teleportation

- TRANSMITTER  $T$  AND RECEIVER  $R$  SHARE ENTANGLED QUBITS

$$|\psi\rangle_{TR} = (|0\rangle_T|1\rangle_R - |1\rangle_T|0\rangle_R) / \sqrt{2}$$

- TRANSMITTER ACCEPTS INPUT QUBIT  $|\Psi\rangle_{in} = \alpha|0\rangle_{in} + \beta|1\rangle_{in}$

- TRANSMITTER/RECEIVER/INPUT STATE IN BELL BASIS:

$$\begin{aligned} |\Psi\rangle_{in}|\psi\rangle_{TR} &= (\alpha|0\rangle_R + \beta|1\rangle_R) (|1\rangle_{in}|0\rangle_T - |0\rangle_{in}|1\rangle_T) / \sqrt{8} \\ &+ (\alpha|0\rangle_R - \beta|1\rangle_R) (|1\rangle_{in}|0\rangle_T + |0\rangle_{in}|1\rangle_T) / \sqrt{8} \\ &+ (\alpha|1\rangle_R + \beta|0\rangle_R) (|1\rangle_{in}|1\rangle_T - |0\rangle_{in}|0\rangle_T) / \sqrt{8} \\ &- (\alpha|0\rangle_R - \beta|1\rangle_R) (|1\rangle_{in}|1\rangle_T + |0\rangle_{in}|0\rangle_T) / \sqrt{8} \end{aligned}$$

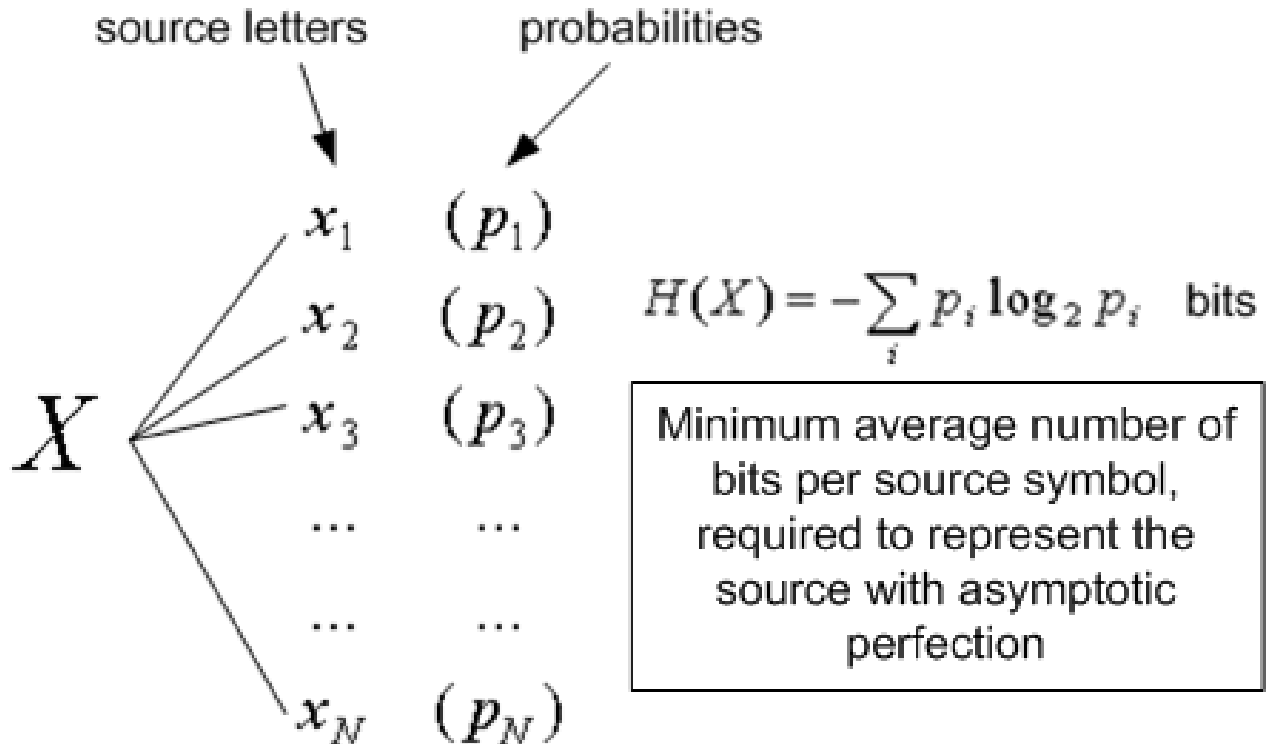
- BELL-STATE MEASUREMENTS MADE ON TRANSMITTER/INPUT
- TWO CLASSICAL BITS SENT TO RECEIVER
- SIMPLE TRANSFORMATION YIELDS  $|\Psi\rangle_R = \alpha|0\rangle_R + \beta|1\rangle_R$

# Quantum Communication and Information Theory

- Classical Information: Shannon Theory

Shannon, Claude E. *A Mathematical theory of communications* Bell System Technical Journal, Vol. 27, pp. 379-423 (part one), pp623-656 (part two), Oct. 1948.

- Source Coding : Data Compression



# Quantum Communication and Information Theory

- Channel Coding : Error Correction and Capacity

Input Alphabet

$X$

$x_1$

$x_2$

$x_3$

...

...

$x_N$

Output Alphabet

$Y$

$y_1$

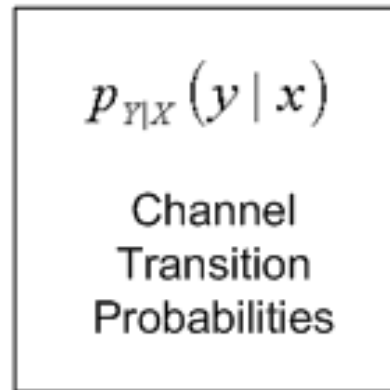
$y_2$

$y_3$

...

...

$y_M$



Mutual Information

$$I(X; Y) = H(X) - H(X|Y)$$

Channel Capacity

$$C = \max_{p_X(x)} I(X; Y)$$

Maximum number of bits that can be sent reliably per use of the channel.

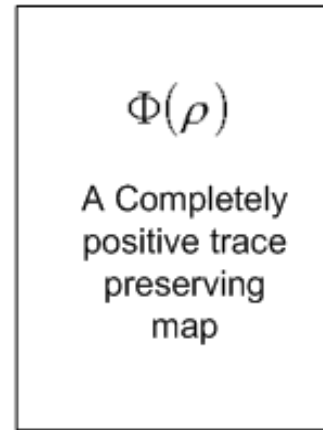
# Quantum Communication and Information Theory

- Quantum Channels
  - Von Neumann Entropy

$$\Pr(i) = p_N(i)$$

$$i = 1, 2, 3, \dots, N$$

$\rho_i$  : Quantum State used to encode source symbol 'i'



Decision Rule or POVM

$$X = \{X_1, X_2, \dots, X_M\}$$

(Complete set of bounded non-negative Hermitian Operators)

$$P(j|i) = \text{Tr}(\Phi(\rho_i)X_j)$$

Classical Transition Probabilities

$$I(p_N, \Phi, X) = \sum_j \sum_i p_N(i) P(j|i) \log \left( \frac{P(j|i)}{\sum_k p_N(k) P(j|k)} \right)$$

$$\Delta H(p_N, \Phi) = S \left( \sum_i p_N(i) \hat{\rho}_i \right) - \sum_i p_N(i) S(\hat{\rho}_i)$$

$$C_n(\Phi) = \sup_{\{p_N(i)\}} \sup_X I(p_N, \Phi^{\otimes n}, X)$$

$$\bar{C}_n(\Phi) = \sup_{\{p_N(i)\}} \Delta H(p_N, \Phi^{\otimes n})$$

$\Phi^{\otimes n} = \Phi \otimes \Phi \otimes \dots \otimes \Phi$  represents multiple uses of the channel

$$\sup_X I(p_N, \Phi^{\otimes n}, X) \leq \Delta H(p_N, \Phi^{\otimes n})$$

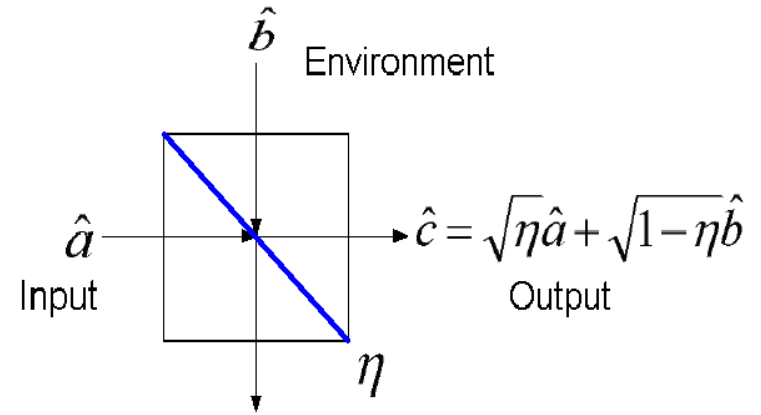
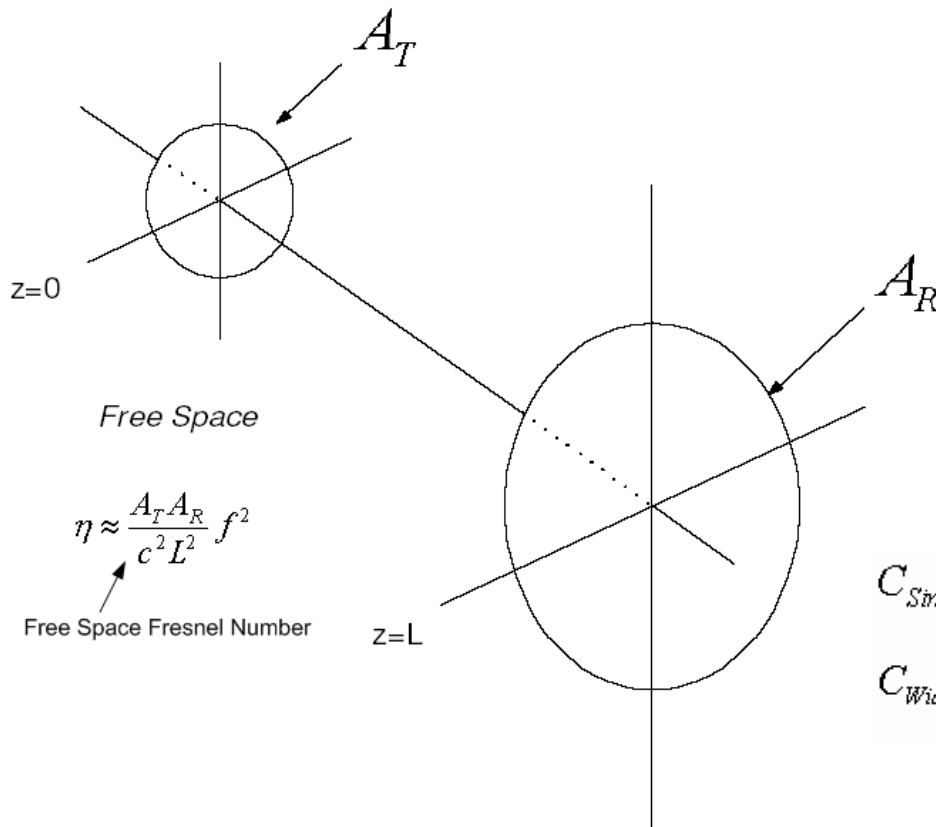
$$S(\rho) = -\text{Tr}(\rho \log \rho)$$

$$C_{CQ} = \bar{C}_1(\Phi)$$

$$C = C_{QQ} = \sup_n \frac{\bar{C}_n(\Phi)}{n}$$

# Quantum Communication and Information Theory

- Free-Space Far-Field Quantum Optical Communication



$$C_{\text{Single-Mode}} = g(\eta \bar{n}) = (1 + \eta \bar{n}) \log(1 + \eta \bar{n}) - \eta \bar{n} \log \eta \bar{n}$$

$$C_{\text{Wide-Band}} = \frac{\pi}{\ln 2} \sqrt{\frac{2\eta P}{3h}}$$

# MIT-NU Long Distance Teleportation Architecture

- **Quantum superposition and quantum entanglement are the bedrock on which new theoretical paradigms for information transmission, storage, and processing are being built. The preeminent obstacle to the development of quantum information technology is the difficulty of transmitting quantum information over noisy and lossy quantum communication channels, recovering and refreshing the quantum information that is received, and then storing it in a reliable quantum memory.**
- **With support from the Multidisciplinary Research Program of the University Research Initiative (MURI), we have assembled a truly interdisciplinary team from researchers at MIT and Northwestern University to overcome this obstacle. The focus of our program is an architecture we have established for long-distance, high-fidelity qubit teleportation. Its key elements are:**
  - ultrabright, narrowband sources of polarization-entangled photon pairs;
  - long-distance transmission of entangled photons over standard telecom fiber;
  - qubit storage and processing in trapped atom quantum memories.

# References

- Nielsen, M. A., Chuang, I. L. *Quantum Computation and Quantum Information* Cambridge University Press, 2000.
- Yuen, H. P., Shapiro, J. H. *Optical Communication with Two-Photon Coherent States-Part I: Quantum-State Propagation and Quantum-Noise Reduction*. IEEE Transactions on Information Theory, Vol 24, No. 6, pp. 657-668, Nov. 1978.
- Mandel, L., Wolf, E. *Optical Coherence and Quantum Optics* Cambridge University Press, 1995
- Caves, C. M., Drummond, P. D. *Quantum Limits on Bosonic Communication Rates* Rev. of Mod. Physics. vol. 66, pp. 481-537, 1994.
- Giovannetti, V., Lloyd, S., Maccone L., Shor, P. W. *Broadband Channel Capacities*, eprint arXiv:quant-ph/0307098 v1, July 14,2003.
- V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen, *Classical Capacity of the lossy bosonic channel: the exact solution*, Phys. Rev. Lett. 92, 027902 (January 15, 2004).