

QUANTUM INFORMATION

INTRODUCTION

The quantum-classical border:

you can't go two ways in the same time;

*an electron can: that is called a
SUPERPOSITION.*

Quantum computer – a **fairy tale** device,
with **existing** small (~10 bit) models

experiment

theory

QUBIT = superposition of YES and NO

$\alpha|0\rangle + \beta|1\rangle$ **coherent**

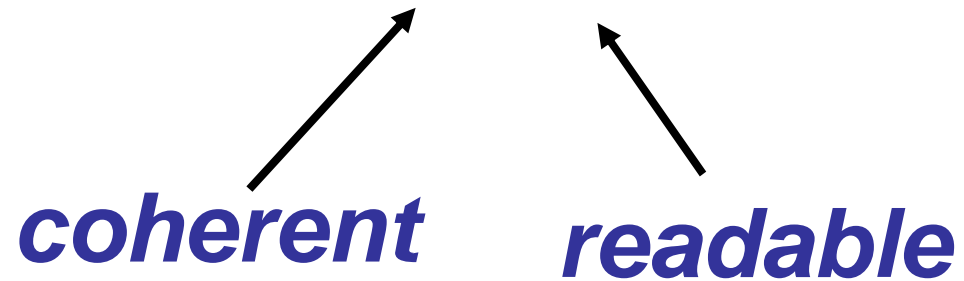
(~analog computation)

MANY QUBITS = a common, **ENTANGLED**
quantum state, **and still coherent!!**

3-state superposition: QUTRIT

d-state superposition: QUDIT

The physical carriers are **MESOSCOPIC** systems



The main difficulty:

- strong interaction inside
(→ speed of operation)
- weak interaction with the environment
(→ to preserve coherence)

WAY OUT: error-correcting algorithms,
environment control
etc ...

Which coherent mesoscopic systems?

2-level systems, manipulated by resonant radiation:

- out of more than 2 levels, 2 can be selectively manipulated and read out by **very sharp resonances, i.e. very long-lived states**
- spontaneous emission is a source of noise; a way out is **slow adiabatic population transfer**

QUANTUM OPTICAL SYSTEMS:

- trapped cold ions and atoms + lasers
- flying atoms + visible-to-microwave photons in a resonator
- “pure” optics: photon polarization + spatial modes

NUCLEAR MAGNETIC RESONANCE

- macroscopic, room-temperature samples: doubtful in matters of entanglement
- complicated protocols of manipulation and readout
- promising for few (<100) qubits, impossible for more

SCALING-UP? war against decoherence

SOLID-STATE SYSTEMS are scalable in principle, hard to make coherent in practice. However, very promising starts...

- semiconductors: quantum dots, single impurities; charge and spin
- superconductors: charge qubits, flux qubits

MICROTRAPS: quantum optics on CHIPS!

WHY QUANTUM COMPUTING?

FEYNMANN 1982: **efficient** simulation of quantum systems

DEUTSCH 1985: quantum computer more **efficient** in tackling hard problems

SHOR 1994:

- factoring prime numbers
- „discrete logarithm”

GROVER 1997: database search

(1969)1984: QUANTUM CRYPTOGRAPHY!

THE BASIC STRATEGY:

QUANTUM LOGICAL
GATES



- compute by approximate **UNITARY EVOLUTION** as long as you can, then read the result by **QUANTUM MEASUREMENT**;
- repeat many times to get **GOOD STATISTICS**

ALTERNATIVE STRATEGIES:

interrupt unitary evolution by quantum measurements

- Linear Optics Quantum Computing
- Cluster State Quantum Computing

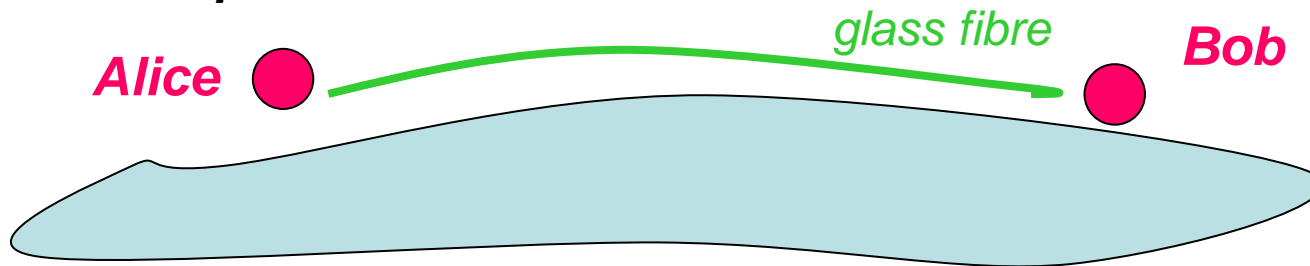
WHAT ARE THE ADVANTAGES?

qubit-qubit coupling in unitary evolution
needs strong **NONLINEARITIES** in the Hamiltonian;
with quantum measurements **WHILE COMPUTING**,
you get strong nonlinearities **FREE!**

Distributing a secret key 01110100110...

encoded into polarizations of **single photons**:

observing them is a **quantum measurement** that would leave a trace on photon statistics



• Alice sends a bit sequence through her randomly chosen polarizers



• Bob observes it through his randomly chosen polarizers



• Through public phone, they select the cases of equal polarizer setting

• Register the corresponding bits and use them as the code

1 1 1 0

• Sacrifice part of the code to detect corruption by **eavesdropping**

How to send qubits (photons)?

1) through optical fibres, 2) through free space.

*advantages,
disadvantages?*

>>>What is needed?

photon sources, transmission, detectors

FREE SPACE:

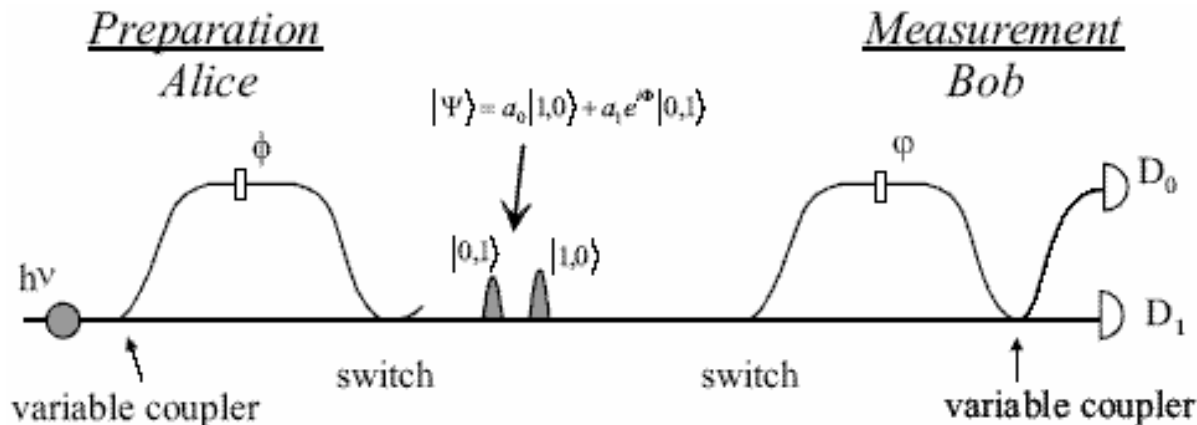
- Transmission disturbed by bad weather and/or geometric obstacles
- Good transmission AND good detectors around 780 nm
- Stable polarization, good for qubit encoding

*polarized starlight, following
6000 yrs space travel...*

OPTICAL FIBRES:

- Good transmission around 1300 or 1550 nm BUT poor detectors there
- Existing telecom networks: no direct visibility needed
- Polarization diffusion:
DIFFERENT QUBIT ENCODING
NEEDED!

**TIME-BIN QUBIT
ENCODING**



OTHER ISSUES OF PRIVACY AMPLIFICATION

- quantum money
- secret sharing in the form of entangled quantum systems, to handle limited confidence

EXAMPLES:

- 1) police detect ***if my car is stolen***, but cannot find it until I give them access to my part of information
- 2) Alice and Bob are both shy and afraid of being refused. To decide ***if they should have a date***: if they both send a YES, they will learn it; if not, the one who says no, does not learn what the other has said

qubit orthography

1-qubit basis:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

a 1-qubit superposition:

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

2-qubit basis:

$$|00\rangle \equiv |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|01\rangle \equiv |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|10\rangle \equiv |2\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$|11\rangle \equiv |3\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

the rule:

$$|00101111001000101\dots\rangle \equiv |x\rangle; \quad x = \sum_{i=0}^{n-1} a_i 2^i$$

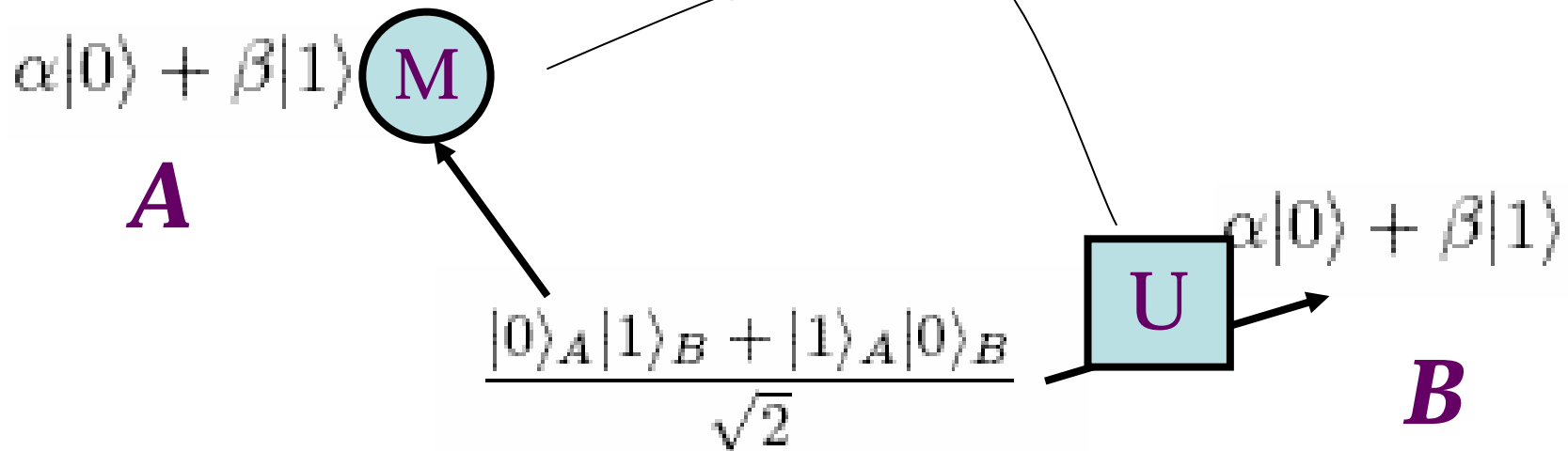
CLONING, NON-CLONING

$$\begin{array}{l}
 |00\rangle \rightarrow |00\rangle \\
 |01\rangle \rightarrow |00\rangle \\
 |10\rangle \rightarrow |11\rangle \\
 |11\rangle \rightarrow |11\rangle
 \end{array}
 \begin{pmatrix}
 1 & 1 & 0 & 0 \\
 0 & 0 & 0 & 0 \\
 0 & 0 & 0 & 0 \\
 0 & 0 & 1 & 1
 \end{pmatrix}$$

- It is a PROJECTOR:
it is not unitary
- It does not clone a superposition

The no-cloning theorem

TELEPORTATION



LOCC: Local Operation with Classical Communication –
an early, evergreen example of Unitarity interrupted by Quantum Measurement

SHOR'S FACTORIZING ALGORITHM

To factorize integer N , choose another integer a , relative prime to N , and introduce

$$f_{a,N}(x) = a^x \pmod N$$

This function is periodic in x . Let its period length be r , then two divisors of N are

$$\gcd(a^{r/2} \pm 1, N)$$

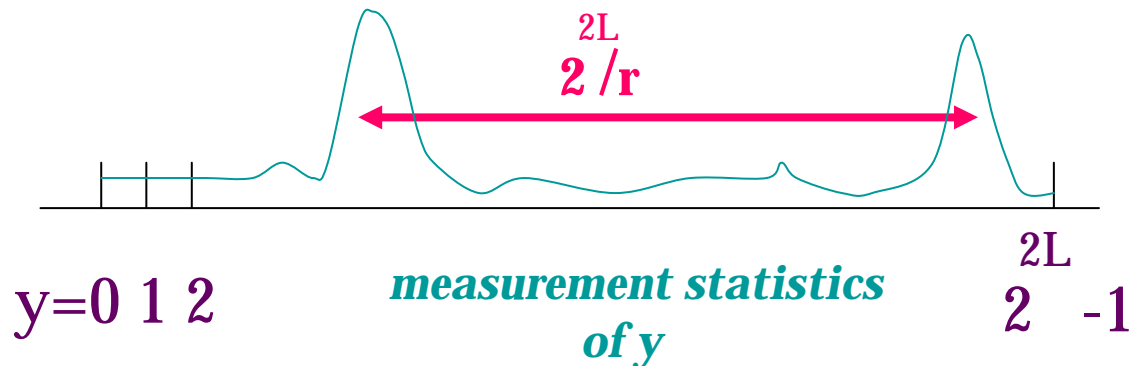
Rev. Mod. Phys. 68, 733 ('96)

HOW TO MEASURE r ?

by QUANTUM FOURIER TRANSFORM (using 1- and 2-qubit gates)

$$\Psi = \sum_{x=0}^{2^N-1} f_{a,N}(x) |x\rangle \xrightarrow{\text{F.F.T.}} c_y = 2^{-L} \sum_{x=0}^{2^{2L}-1} \exp(2\pi ixy/2^{2L}) c_x$$

L : length of integer N ; $2L$ long quantum register needed




quantum logical gates = **elementary unitary transforms**, building blocks of algorithms

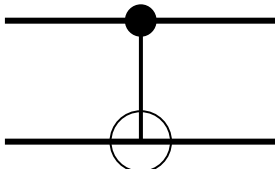
1-QUBIT GATES

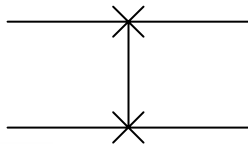
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{The „Pauli gates”,}$$

X is the NOT gate!

HADAMARD gate $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ 

2-QUBIT GATES

CNOT (controlled-NOT) $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$  $\begin{matrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{matrix}$

SWAP („controlled phase”) gate  $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

$$H^{\otimes n} |000000\dots 0\rangle = 2^{-n/2} \sum_{x=0}^{2^n-1} |x\rangle \quad \text{to initialize a computation}$$

IMPORTANT: $H^{\otimes n} |x\rangle = 2^{-n/2} \sum_{y=0}^{2^n-1} (-1)^{\vec{x} \cdot \vec{y}} |y\rangle$ **WHY?**

*bitwise
scalar
product*

GROVER'S SEARCH ALGORITHM

computer chess: which move is best?

S_1, S_2, \dots, S_N : n-bit strings ($N = 2^n$)

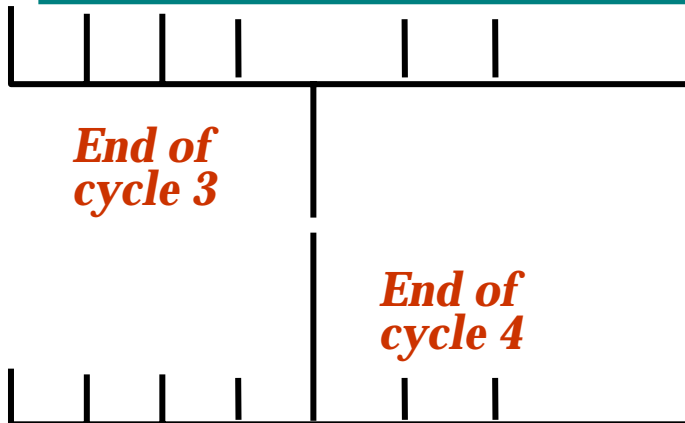
search for S_v satisfying condition $C(S) = 1$ for $S = S_v$, else $C(S) = 0$

- Encode bit strings into qubit strings $|x\rangle$;
- Initialize q-computer as above;
- do working cycle many times, to enforce evolution of $|\Psi\rangle = \sum_{x=0}^{2^n-1} c_x |x\rangle$:

QUANTUM PARALLELISM AT WORK: SIMULTANEOUS PROCESSING OF ALL TERMS OF THE SUPERPOSITION

1. Do $c_v \rightarrow -c_v$ for the winner amplitude, leaving the rest untouched;
2. Do $c_x \rightarrow \sum_y D_{xy} c_y$ for ALL amplitudes, with:

$$D_{xy} = \begin{cases} 2/N & \text{for } x \neq y, \\ (-1 + 2/N) & \text{for } x = y. \end{cases}$$
3. Repeat as long as appropriate (!);
4. Measure the quantum state obtained to find largest amplitude c_v



**Winner reaches maximum size $O(1)$
in \sqrt{N} steps,
then gradually sinks back to nothing**

proof of step 2. based on Hadamard gates

ERROR-CORRECTING ALGORITHMS

necessary, because of **decoherence** → quantum phase errors

bit errors are easy to correct: use **MULTIPLE ENCODING**

$$|0\rangle \rightarrow |000\rangle, \quad |1\rangle \rightarrow |111\rangle$$

the “true bit”

the “ANCILLAS”

Errors in the true bit can be easily corrected:

$$1) \text{ CNOT } \begin{array}{l} 1 \swarrow 2 \\ \searrow 3 \end{array} \begin{array}{l} |100\rangle \rightarrow |111\rangle \\ |011\rangle \rightarrow |011\rangle \end{array}$$

$$2) \text{ TOFFOLI } \begin{array}{l} 2 \swarrow 1 \\ \searrow 3 \end{array} \begin{array}{l} |111\rangle \rightarrow |011\rangle \\ |011\rangle \rightarrow |111\rangle \end{array} \\ = \text{doubly-CNOT}$$

the tough thing: phase errors

can be tamed by PROTECTIVE CODING, using the HADAMARD gate

which converts phase errors into bit errors:

$$|+\rangle = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \rightarrow \begin{pmatrix} e^{-i\Theta} \\ e^{i\Theta} \end{pmatrix}$$

$$\begin{array}{l} |0\rangle \rightarrow |+\rangle = (|0\rangle + |1\rangle)/\sqrt{2} \\ |1\rangle \rightarrow |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2} \end{array}$$

$$\approx \begin{pmatrix} 1 \\ 1 \end{pmatrix} - i\Theta \begin{pmatrix} 1 \\ -1 \end{pmatrix} = |+\rangle - i\Theta|-\rangle$$

Finally, back from + and - to 0 and 1, and correct bit error

SUMMARY

- Quantum information took a promising start
- Cryptography and other privacy amplification procedures keep it alive and prosperous
- Useful quantum computers are still a dream
- Nevertheless, developing parts for the still non-existing quantum computers is great fun, in physics and technology, in theory and experiment
- Quantum information theory is beautiful, offering unexpected insight to Quantum Physics of Nature

WHAT TO READ?

**The basic reference is: M. A. Nielsen and I. L. Chuang:
Quantum Computation and Quantum Information,
Cambridge University Press 2000**

READ IT, THEN ASK AGAIN...