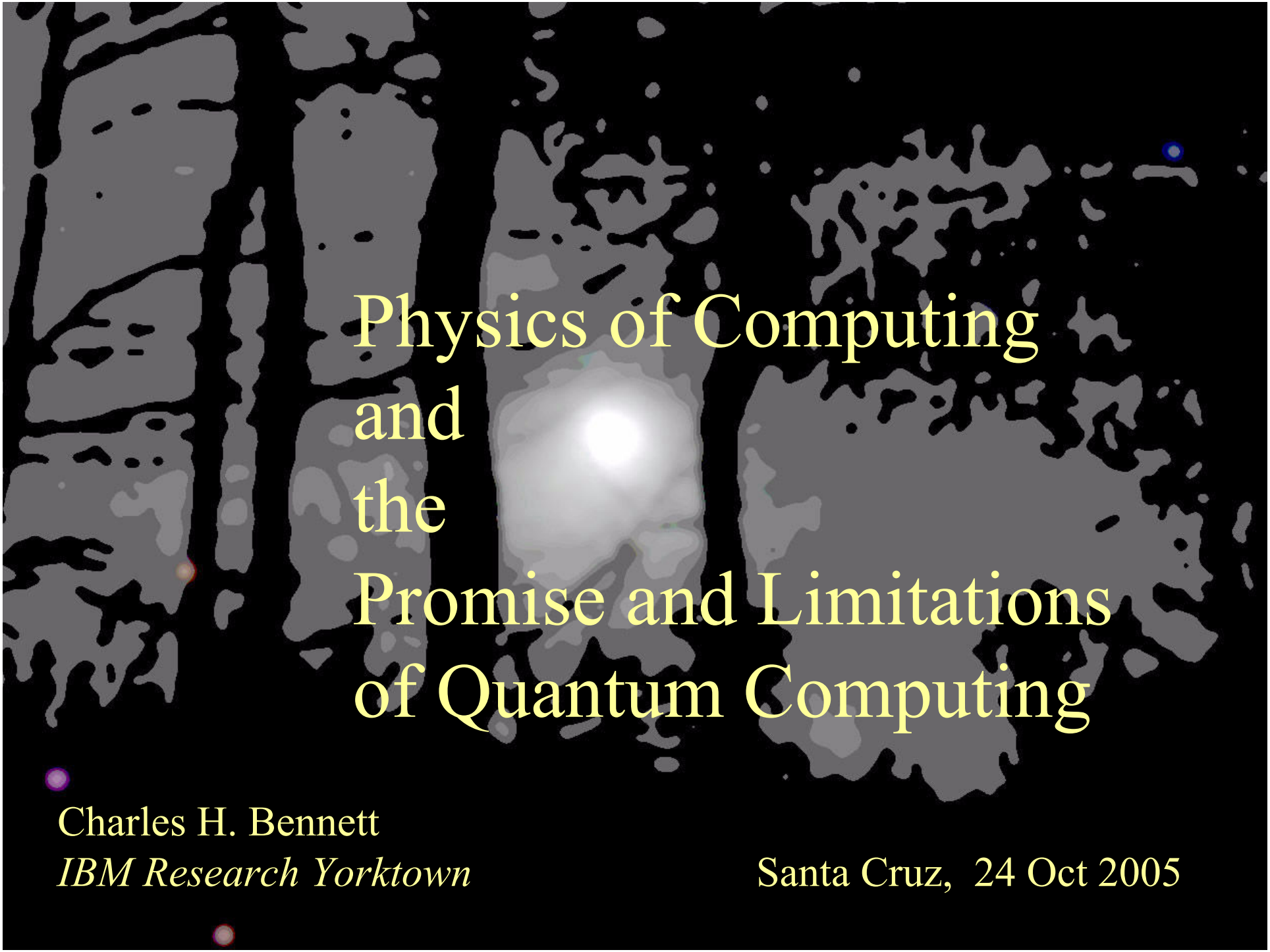


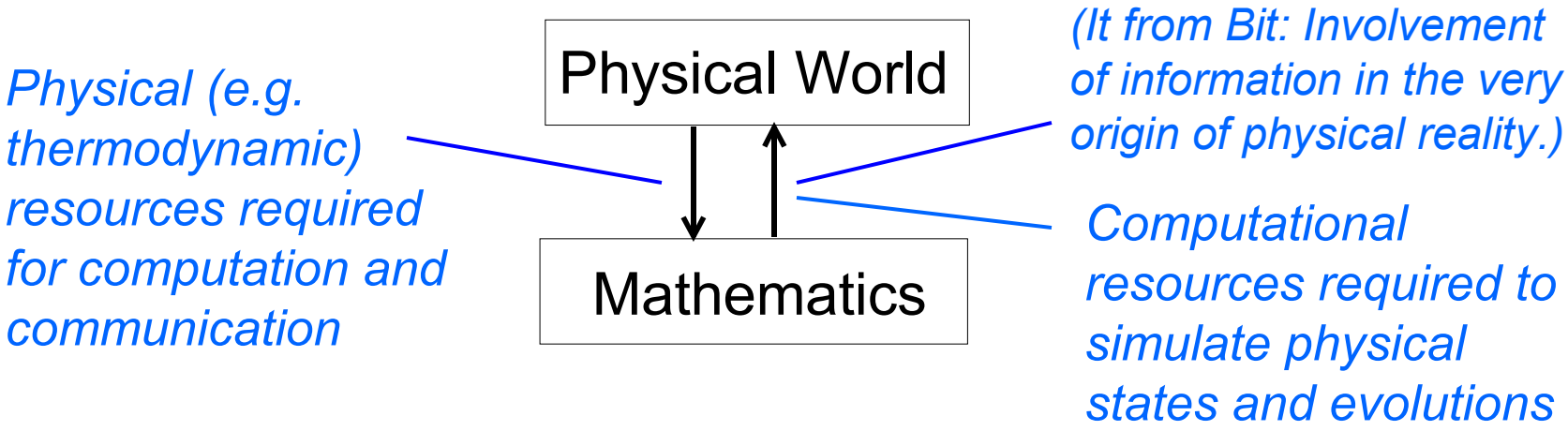
Physics of Computing and the Promise and Limitations of Quantum Computing

Charles H. Bennett
IBM Research Yorktown

Santa Cruz, 24 Oct 2005

"Information is Physical" Rolf Landauer

"It from bit" John Archibald Wheeler



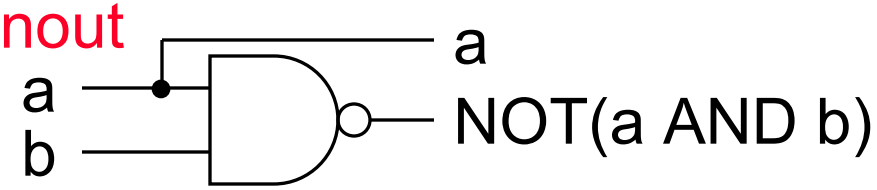
When Turing, Shannon, von Neumann and their contemporaries formalized the notions of information and computation, they left out notions of reversibility and quantum superposition

reversibility => thermodynamics of computation

superposition => quantum information/computation theory.

Conventional computer logic uses irreversible gates, eg NAND, but these can be simulated by reversible gates. Toffoli gate is universal.

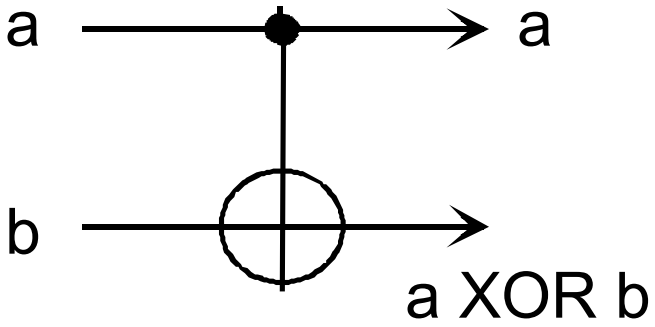
Fanout



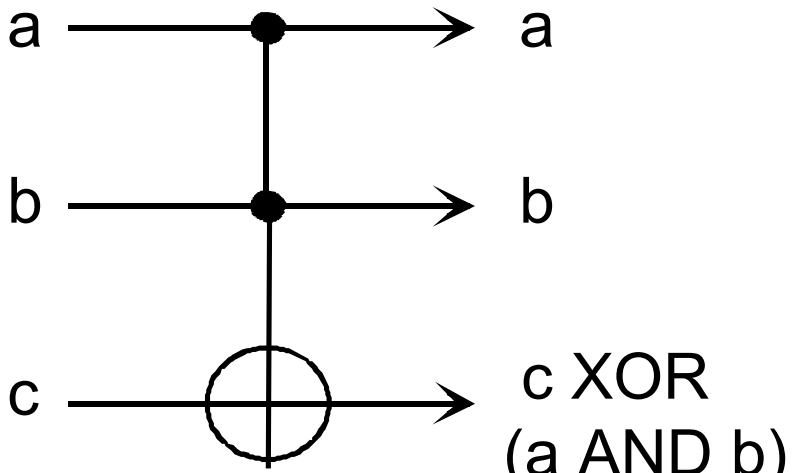
NAND gate

no inverse

Reversible logic was used to show that computation is thermodynamically reversible in principle. Now it is needed for quantum computation.



XOR gate



Toffoli gate

self-inverse

Information = Distinguishability,
considered as an abstract property separate from the physical information carrier.
(Using a pencil, a piece of paper can be put into various states distinguishable at a later time.)

- Information is reducible to bits (**0** ,**1**)

- Information processing, to reveal implicit truths, can be reduced to logic gates (**NOT**, **AND**)

- bits and gates are *fungible*, independent of physical embodiment, making possible Moore's law

We take for granted that information
- can be copied without disturbing it
- cannot travel faster than light
- can be erased when no longer wanted

But chemists and physicists have long known that

Information in microsopic bodies such as photons or nuclear spins obeys quantum laws. Such information

- cannot be read or copied without disturbance.

- can connect two spacelike separated observers by a correlation too strong to be explained by classical communication. However, this "entanglement" cannot be used to send a message faster than light or backward in time.

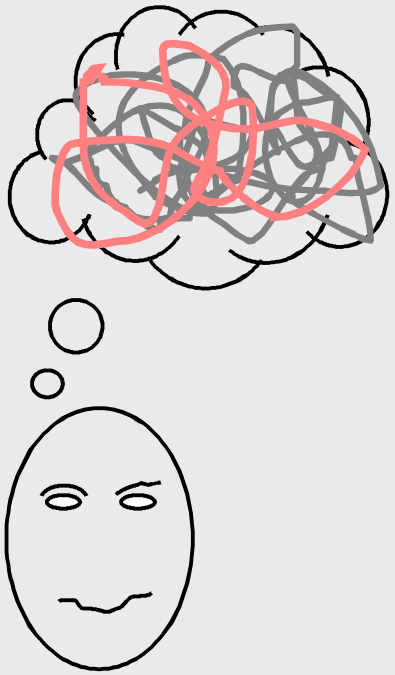
Quantum information is reducible to **qubits** i.e. two-state quantum systems such as a photon's polarization or a spin-1/2 atom.

Quantum information processing is reducible to one- and two-qubit gate operations.

Qubits and quantum gates are fungible among different quantum systems

Ordinary classical information, such as one finds in a book, can be copied at will and is not disturbed by reading it.

Quantum information is more like the information in a dream



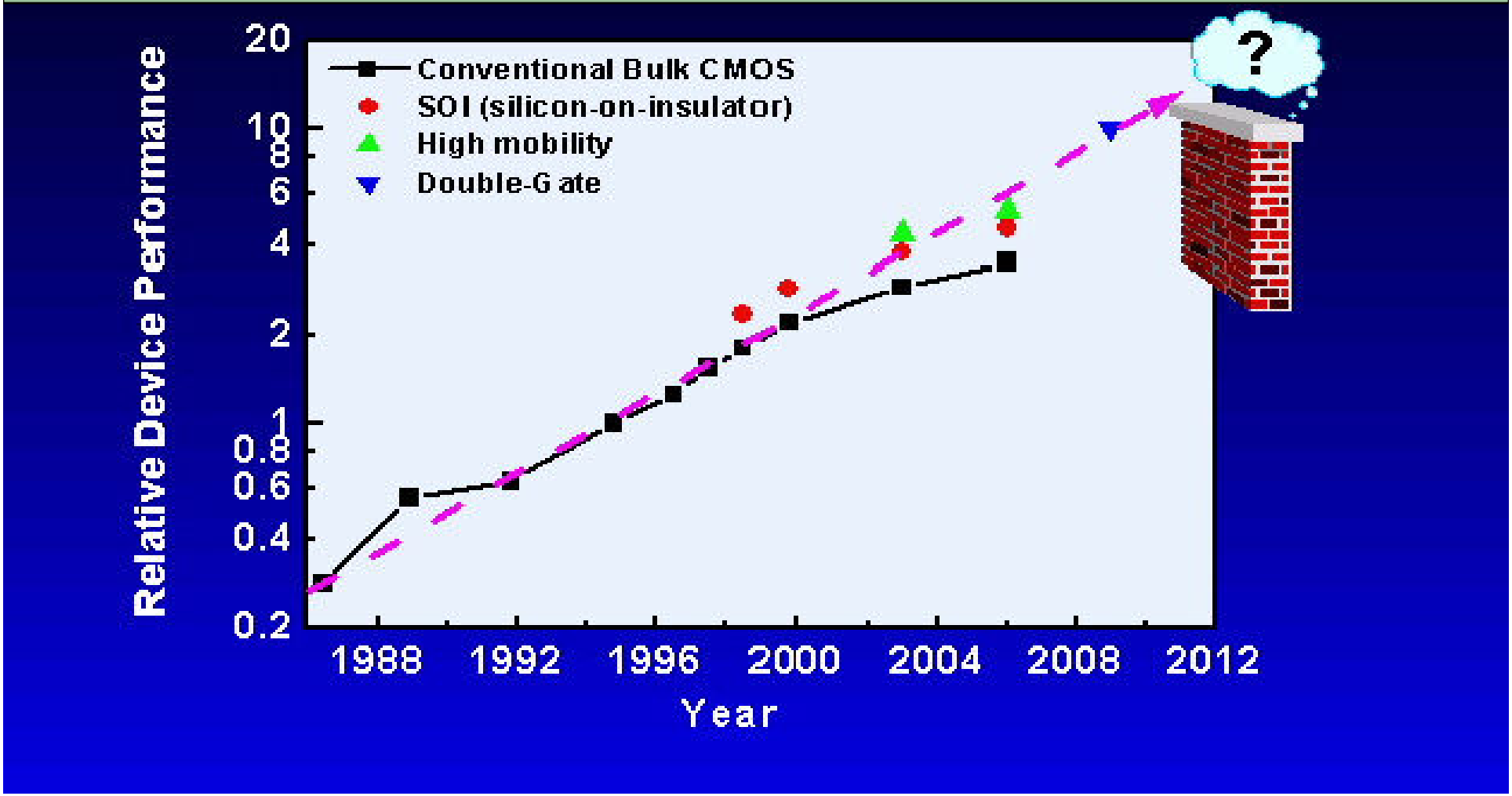
• Trying to describe your dream changes your memory of it, so eventually you forget the dream and remember only what you've said about it.

• You cannot prove to someone else what you dreamed.

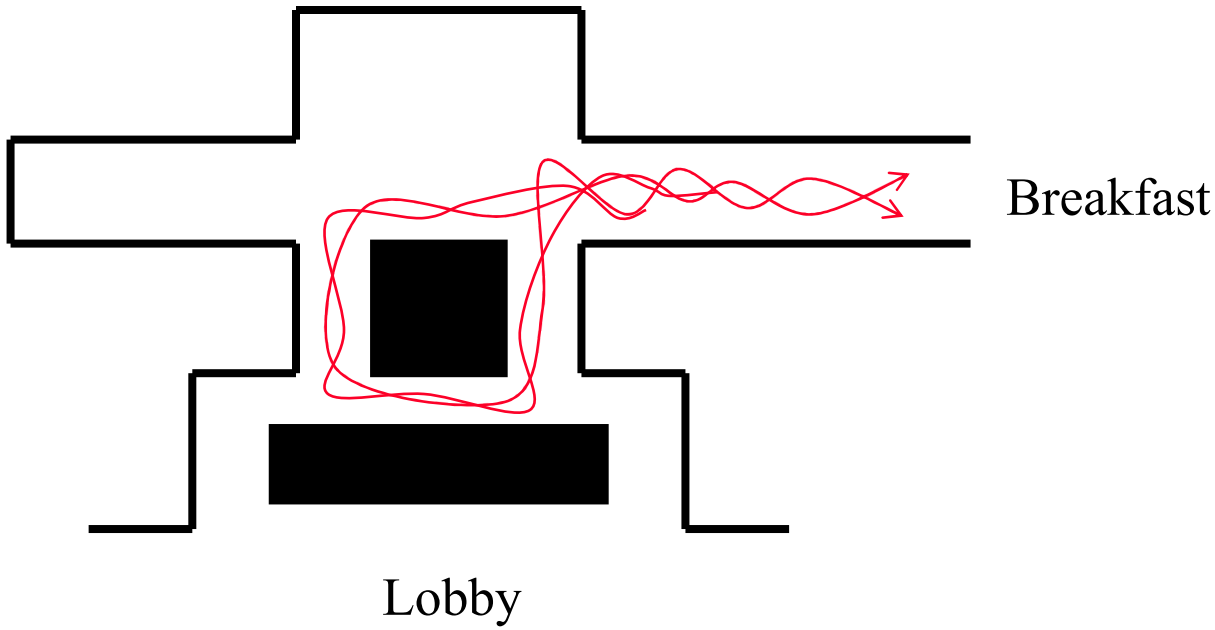
• You can lie about your dream and not get caught.

But unlike dreams, quantum information obeys well-known laws.

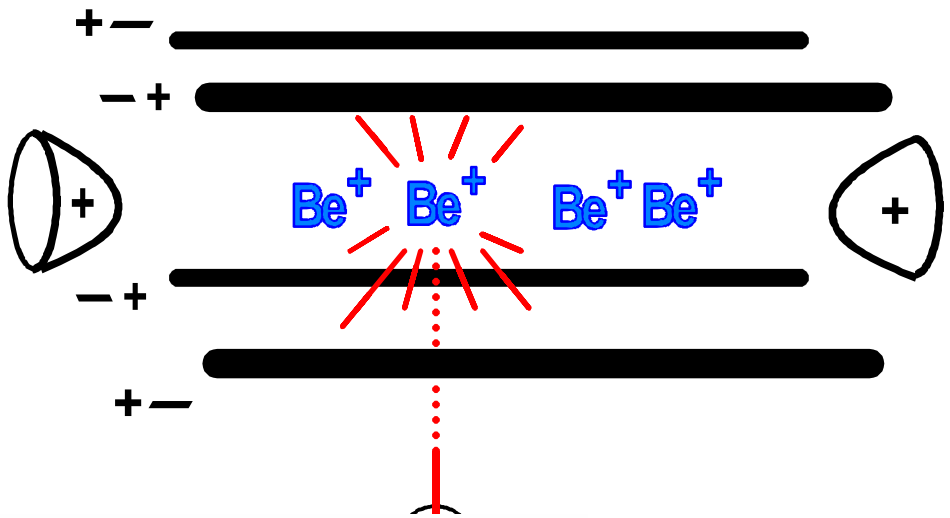
Computer performance has been increasing exponentially for several decades (Moore's law). But this can't go on for ever. Can quantum computers give Moore's law a new lease on life? If so, how soon will we have them?



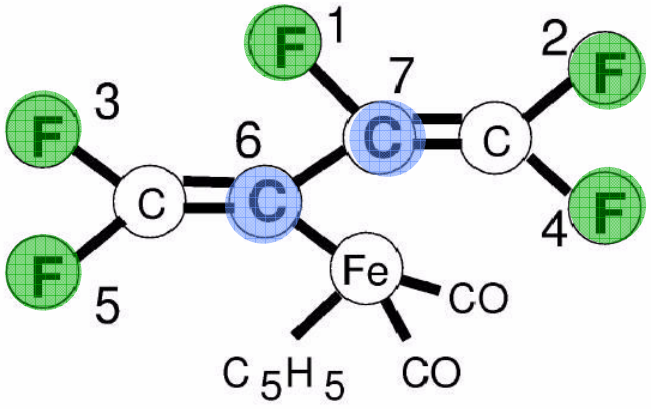
Interference illustrated by back reflection of most people trying to get from Breakfast to Lobby



Some proposed physical implementations of quantum computing



Ion trap: scalable in principle, existing experiments have reached only about ~~2~~ ~~4~~ 5 qubits.



Liquid State NMR: used to implement most complicated computations so far, on several qubits. Significant obstacles to scaling above about 10 qubits.

This 7 qubit molecule was used to factor 15

Physical systems actively considered for quantum computer implementation

- Liquid-state NMR
- NMR spin lattices
- Linear ion-trap spectroscopy
- Neutral-atom optical lattices
- Cavity QED + atoms
- Linear optics with single photons
- Nitrogen vacancies in diamond
- Topological defects in fractional quantum Hall effect systems
- Electrons on liquid helium
- Small Josephson junctions
  - "charge" qubits
  - "flux" qubits
- Spin spectroscopies, impurities in semiconductors
- Coupled quantum dots
  - Qubits: spin, charge, excitons
  - Exchange coupled, cavity coupled

Executive Summary

• A Quantum computer can probably be built eventually, but not right away. Maybe in 20 years. We don't know yet what it will look like.

• It would exponentially speed up a few computations like factoring, thereby breaking currently used digital signatures and public key cryptograp (Shor algorithm)

• Quantum molecular dynamics

• Speedup of many important optimization problems like the traveling salesman, but only quadratically, not exponentially. (Grover algorithm)

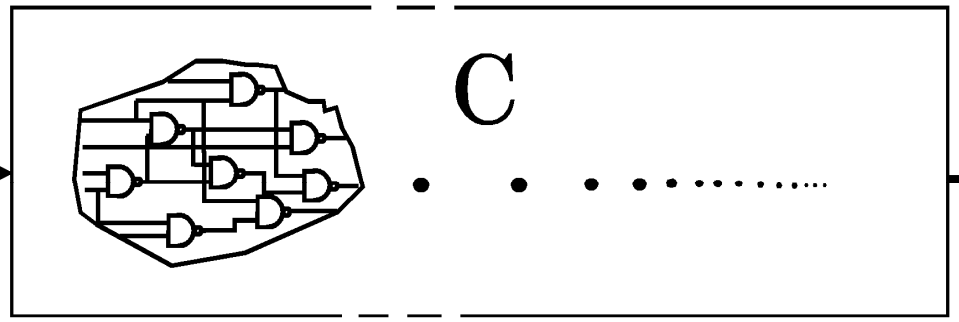
• There would be no speedup for many other problems. For these computational tasks, Moore's law would still come to an end, even with quantum computers.

• Other applications—quantum cryptography, metrology, distributed computation

(For a classical computer, factoring appears to be exponentially harder than multiplication, by the best known algorithms.)

RSA 129

1143816257578888676
6923577997614661201
0218296721242362562
5618429357069352457
3389783059712356395
8705058989075147599
290026879543541



Factors

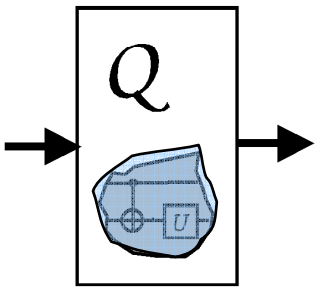
3490529510847650949
1478496199038981334
1776463849338784399
0820577

x

3276913299326670954
9961988190834461413
1776429679929425397
98288533

Same Input and Output, but Quantum processing of intermediate data gives

1143816257578888676
6923577997614661201
0218296721242362562
5618429357069352457
3389783059712356395
8705058989075147599
290026879543541



3490529510847650949
1478496199038981334
1776463849338784399
0820577

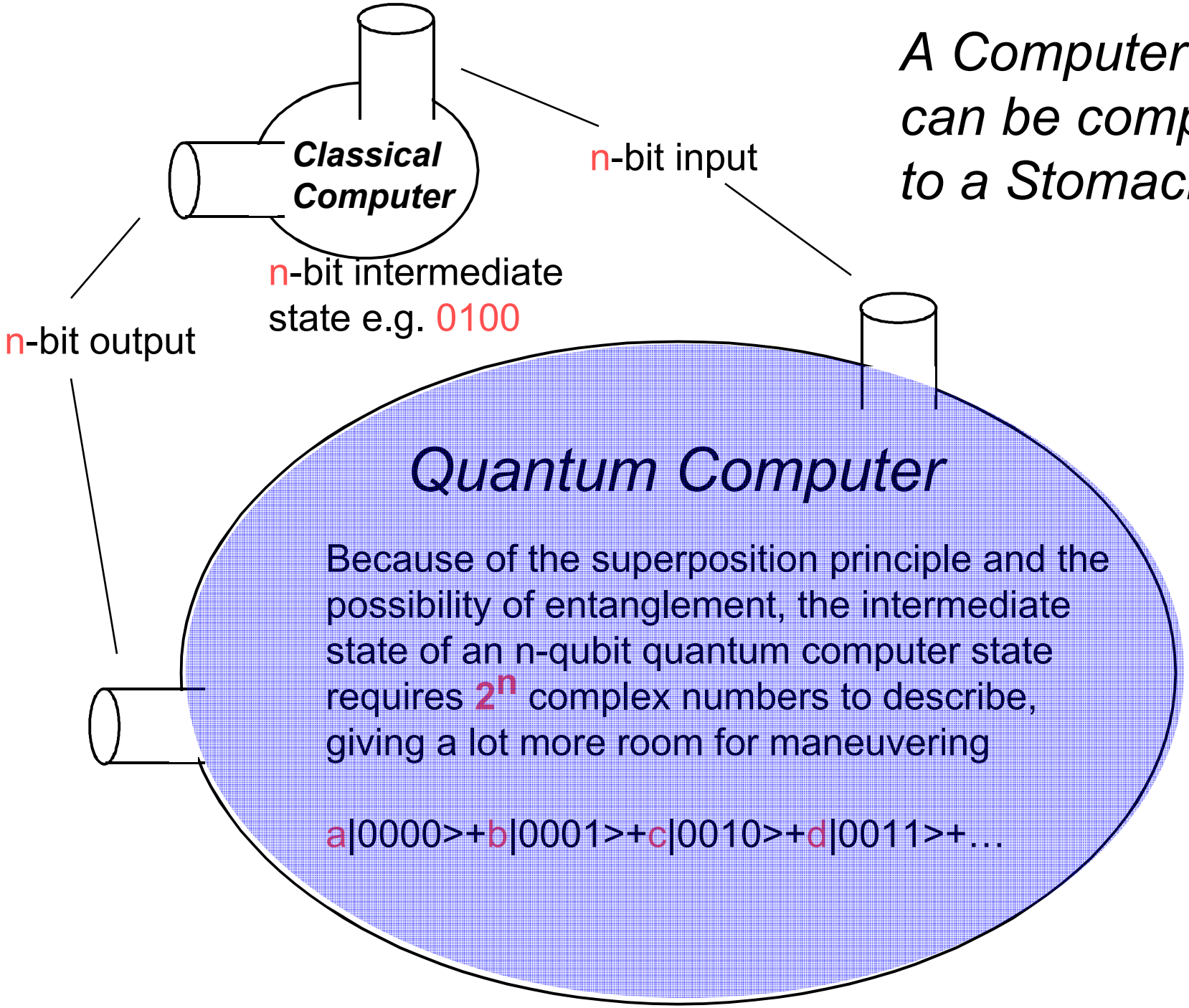
x

3276913299326670954
9961988190834461413
1776429679929425397
98288533

Exponential speedup
for Factoring (Shor algorithm)

Quadratic speedup
for Search (Grover algorithm)

(For a quantum computer, factoring is about as easy as multiplication, due to the availability of **entangled** intermediate states.)



A Computer can be compared to a Stomach

How Much Information is "contained in" n qubits, compared to n classical bits, or n analog variables?

	Digital	Analog	Quantum
Information required to specify a state	n bits	n real numbers	2^n complex numbers
Information extractable from state	n bits	n real numbers	n bits
Good error correction	yes	no	yes

The Downside of Entanglement

Quantum data is exquisitely sensitive to decoherence, a randomization of the quantum computer's internal state caused by entangling interactions with the quantum computer's environment.

Fortunately, decoherence can be prevented, in principle at least, by quantum error correction techniques developed since 1995, including

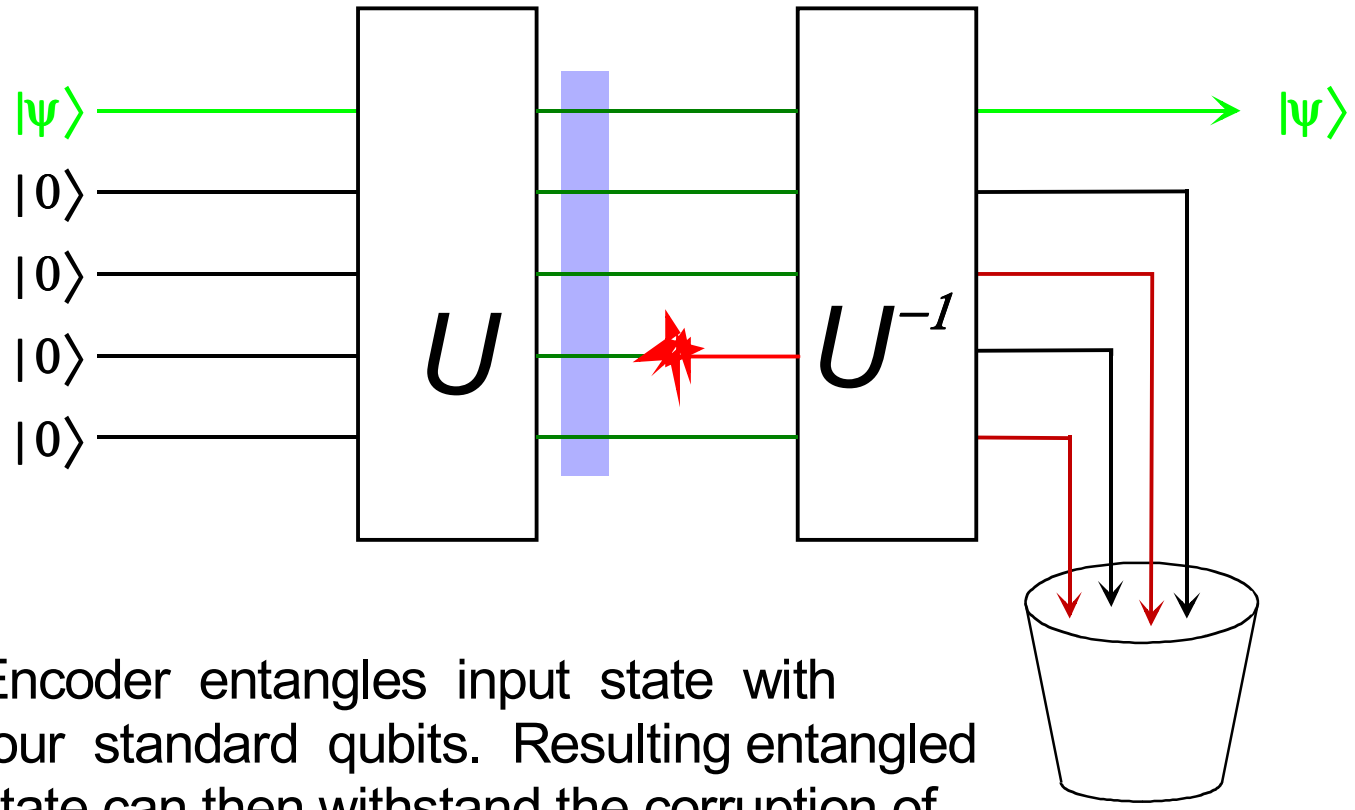
Quantum Error Correcting Codes

Entanglement Distillation

Quantum Fault-Tolerant Circuits

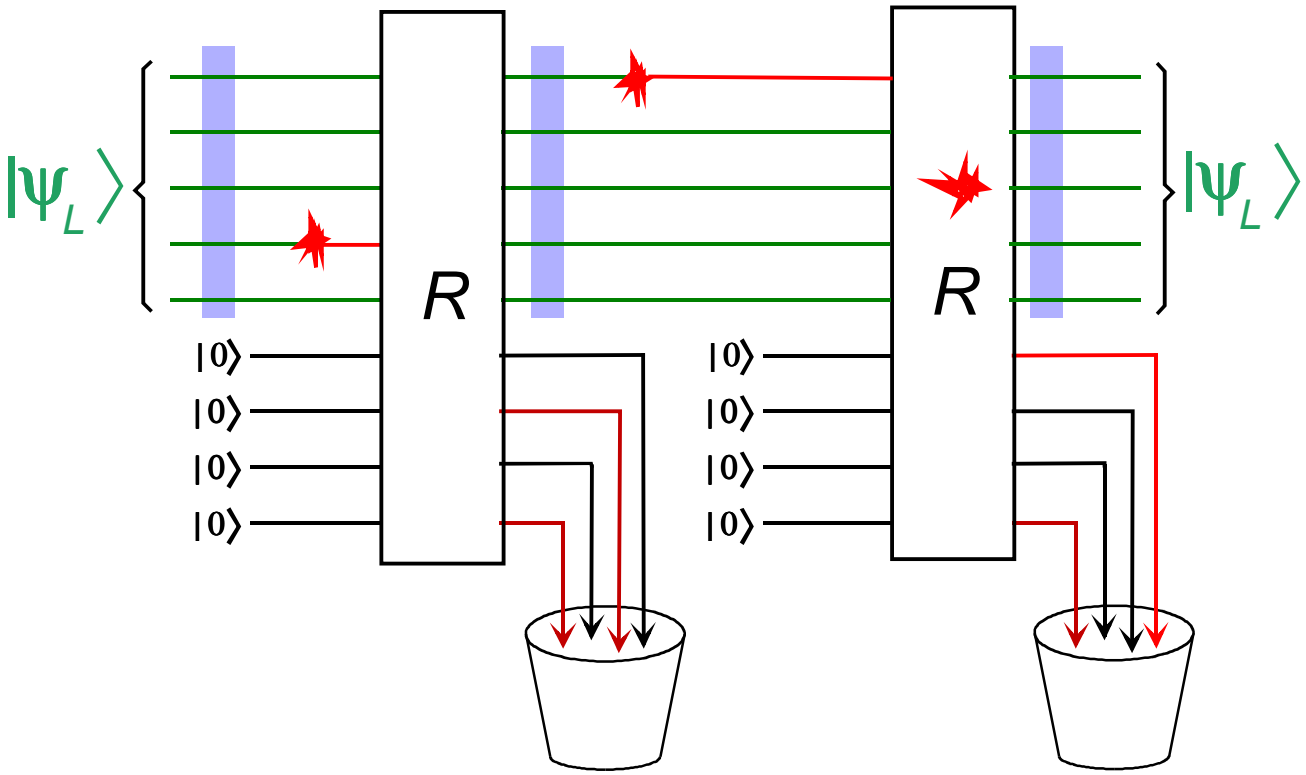
These techniques, combined with hardware improvements, will probably allow practical quantum computers to be built, but not any time soon.

The Simplest Quantum Error-Correcting Code



Encoder entangles input state with four standard qubits. Resulting entangled state can then withstand the corruption of any one of its qubits, and still allow recovery of the exact initial state by a decoder at the receiving end of the channel

Quantum Fault Tolerant Computation



Clean qubits are brought into interaction with the quantum data to siphon off errors, even those that occur during error correction itself.

Thermodynamics of Computation

• Landauer's Principle: each erasure of a bit, or other logical 2:1 mapping of the state of a physical computer, increases the entropy of its environment by k log 2.

• Reversible computers, which by their hardware and programming avoid these logically irreversible operations, can in principle operate with arbitrarily little energy dissipation per step.

Avatars of the Second Law of Thermodynamics:

No physical process has as its sole result is the conversion of heat into work.

It is impossible to extract work from a gas at constant volume if all parts are initially at the same temperature and pressure.

It is impossible to see anything inside a uniformly hot furnace by the light of its own glow.

No physical process has as its sole result the erasure of information.

Looking inside a pottery kiln

by its own glow

by external light