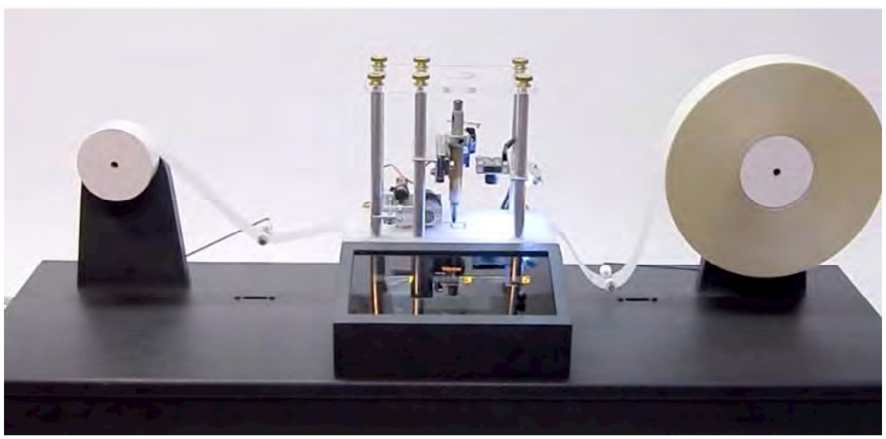
Introduction and Overview (Preskills Notes)

Physics of Information: Turing
von Neumann

Notions: What is a computation ?
What is computable

Formulation of Computer Science that is Device Independent

1937 Turing Machine:



https://www.youtube.com/watch?v=E3keLeMwfHY

Wikipedia:

A Turing Machine (TM) is a mathematical model of computation describing an abstract machine that manipulates symbols on a strip of paper according to a table of rules.

The TM operates on an infinite tape divided into cells, each of which can hold a symbol drawn from a finite set.

At each step the head reads the symbol in the cell. Then, based on the symbol and the TM's present state, the machine writes a symbol in the cell, and moves the head one step to the left or the right, or halts the computation.

https://en.wikipedia.org/wiki/Turing_machine

Church – Turing Thesis:

Everything that is computable can be computed on a Turing Machine with at most polynomial overhead.

Introduction and Overview (Preskills Notes)

Wikipedia:

A Turing Machine (TM) is a mathematical model of computation describing an abstract machine that manipulates symbols on a strip of paper according to a table of rules.

The TM operates on an infinite tape divided into cells, each of which can hold a symbol drawn from a finite set.

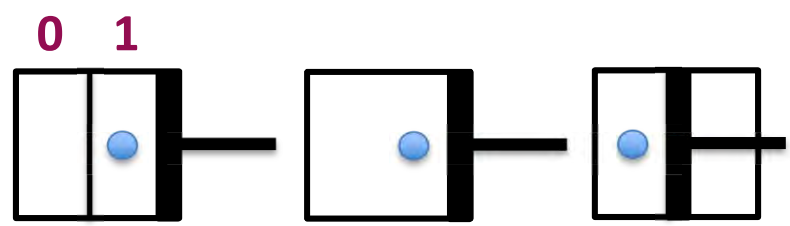
At each step the head reads the symbol in the cell. Then, based on the symbol and the TM's present state, the machine writes a symbol in the cell, and moves the head one step to the left or the right, or halts the computation.

Church – Turing Thesis:

> **Everything that is computable can be computed on a Turing Machine with at most polynomial overhead.**

Landaur: Information is Physical !

Example: Erasure = Dissipation



Entropy: $\Delta S_{gas} = -k \ln 2$

Work: $W = kT \ln 2 = 0.96 \times 10^{-23} \frac{J}{K} \cdot 300K$

$\sim 3 \times 10^{-21} J \sim 0.02 eV$

Is there a way around it ?

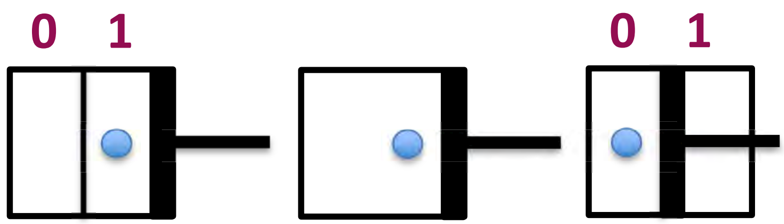
Reversible Computation !

But we need a different gate set !

Introduction and Overview (Preskills Notes)

Landaur: Information is Physical !

Example: Erasure = Dissipation



Entropy: $\Delta S_{gas} = -k \ln 2$

Work: $W = kT \ln 2 = 0.96 \times 10^{-23} \frac{J}{K} \cdot 300K$

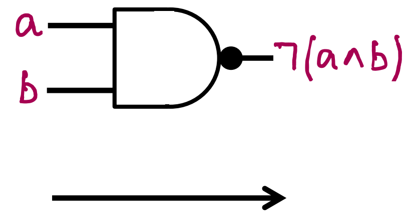
$\sim 3 \times 10^{-21} J \sim 0.02 eV$

Is there a way around it ?

Reversible Computation !

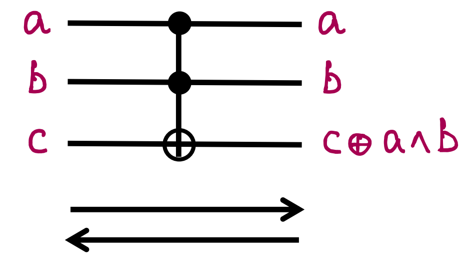
But we need a different gate set !

NAND Gate:



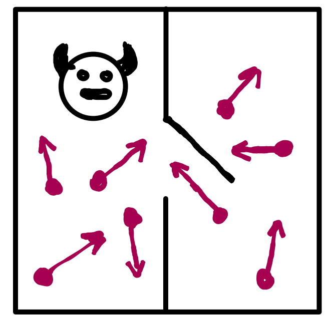
irreversible

Toffoli Gate:



reversible

Maxwells Demon:



Information is Physical !

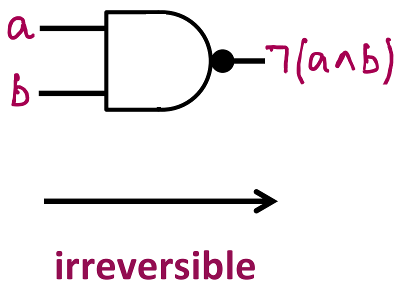
Quantum Information

Carl Caves: Quantum States are states of knowledge

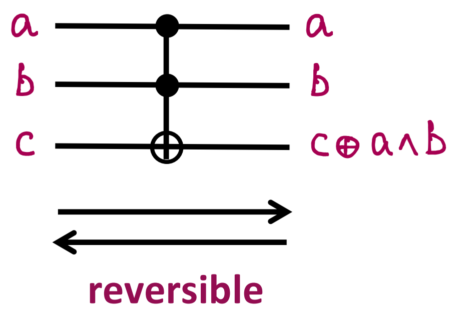
Physics is Information !

Introduction and Overview (Preskills Notes)

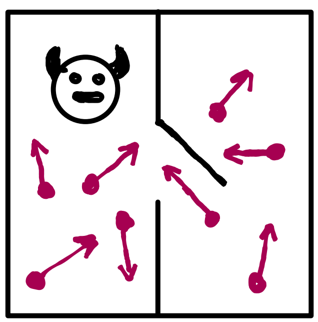
NAND Gate:



Toffoli Gate:



Maxwells Demon:



Information is Physical!

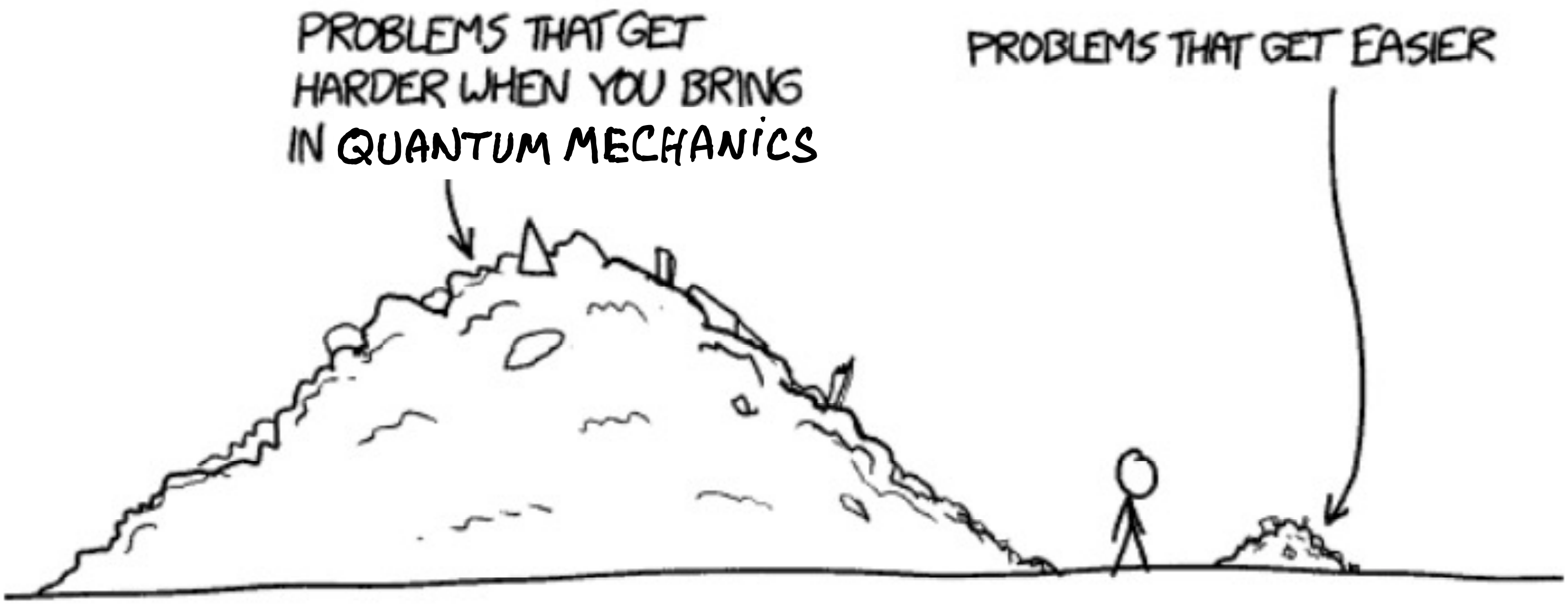
Quantum Information

Carl Caves: Quantum States are states of knowledge

Physics is Information!

New properties of QM

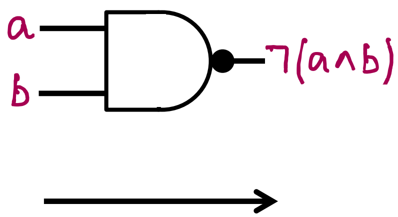
Introduction and Overview (Preskills Notes)



Source: xkcd.com

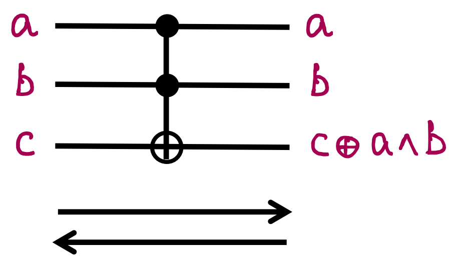
Introduction and Overview (Preskills Notes)

NAND Gate:



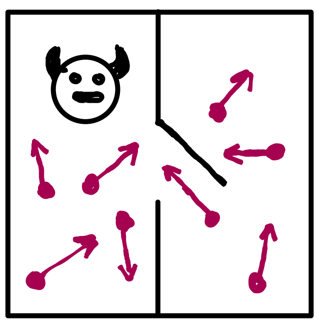
irreversible

Toffoli Gate:



reversible

Maxwells Demon:



Information is Physical !

Quantum Information

Carl Caves: Quantum States are states of knowledge

Physics is Information !

New properties of QM

Measurement:

$$[A,B] \neq 0 \Rightarrow \Delta A \Delta B \geq \frac{\hbar}{2} |\langle [A,B] \rangle|$$

Acquire Info ⇨ Disturb system

Randomness:

Outcome fundamentally unpredictable

"Collapse" of wavefunction

Cannot determine state of a single quantum if initially unknown } Cannot Copy
No cloning theorem

Entanglement:

Non-local correlations

pure state, entangled

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle \right)$$

$$\rho = \frac{1}{2} \left(|00\rangle\langle 00| + |11\rangle\langle 11| \right)$$

mixed state,
not entangled

Introduction and Overview (Preskills Notes)

New properties of QM

Measurement:

$$[A,B] \neq 0 \Rightarrow \Delta A \Delta B \geq \frac{\hbar}{2} |\langle [A,B] \rangle|$$

Acquire Info ⇒ Disturb system

Randomness:

Outcome fundamentally unpredictable

"Collapse" of wavefunction

Cannot determine state of a single quantum if initially unknown } Cannot Copy
No cloning theorem

pure state, entangled

Entanglement:

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle \right)$$

Non-local correlations

$$\rho = \frac{1}{2} \left(|00\rangle\langle 00| + |11\rangle\langle 11| \right)$$

mixed state,
not entangled

Quantum Computing

Does QM impact Computation?

Peter Shor (1994): YES ! ⇒ Quantum Fourier Transform

⇓

Factoring !

DFT on N bits	$O[(2^N)^2]$	steps
FFT on "	$O[N 2^N]$	"
QFT on "	$O[N \log N]$	"

Introduction and Overview (Preskills Notes)

Quantum Computing

Does QM impact Computation?

Peter Shor (1994): YES ! ⇨ Quantum Fourier Transform

⇩

Factoring !

DFT on N bits	$\mathcal{O}[(2^N)^2]$	steps
FFT on "	$\mathcal{O}[N2^N]$	"
QFT on "	$\mathcal{O}[N \operatorname{Log} N]$	"

Efficient Factoring

Factoring $n = p \times q$ ⇨ RSA encryption

large integer → n; p, q ← large prime numbers

- easy to verify solution $\operatorname{Log} n$ steps
- very hard to solve $\mathcal{O}[n]$ steps

⇩

Exponential in # of digits

$\boxed{\text{QFT} \Rightarrow \text{Solvable}}$

Preskill Ch. 1, p. 5-6 $T \propto e^{1.9(\operatorname{Log} n)^{1/3}} e^{(\operatorname{Log}\operatorname{Log} n)^{2/3}}$

Best Classical Algorithm

Introduction and Overview (Preskills Notes)

Quantum Computing

Does QM impact Computation?

Peter Shor (1994): YES ! ⇨ Quantum Fourier Transform

⇩

Factoring !

DFT on N bits	$\mathcal{O}[(2^N)^2]$	steps
FFT on "	$\mathcal{O}[N 2^N]$	"
QFT on "	$\mathcal{O}[N \log N]$	"

Efficient Factoring

Factoring $n = p \times q$ ⇨ RSA encryption

large integer (n) — large prime numbers (p, q)

- easy to verify solution $\log n$ steps
- very hard to solve $\mathcal{O}[n]$ steps

⇩

Exponential in # of digits

QFT ⇨ Solvable

Preskill Ch. 1, p. 5-6 $T \propto e^{1.9(\log n)^{1/3}} e^{(\log \log n)^{2/3}}$

(1998) 130 digits in 1 month

⇩

400 digits in 10^{10} years

(2022) 24 yrs = 16 Moores Law doublings

$2^{16} = 65{,}536$ ⇨ 400 digits ~ 150kYrs

Introduction and Overview (Preskills Notes)

Quantum Computing

Does QM impact Computation?

Peter Shor (1994): YES ! ⇨ Quantum Fourier Transform

⇩

Factoring !

DFT on N bits	$\mathcal{O}[(2^N)^2]$	steps
FFT on "	$\mathcal{O}[N 2^N]$	"
QFT on "	$\mathcal{O}[N \log N]$	"

Efficient Factoring

Factoring $n = p \times q$ ⇨ RSA encryption

large integer (n); large prime numbers (p, q)

- easy to verify solution $\log n$ steps
- very hard to solve $\mathcal{O}[n]$ steps

⇩

Exponential in # of digits

QFT ⇨ Solvable

Preskill Ch. 1, p. 5-6 $T \propto e^{1.9(\log n)^{1/3}} e^{(\log \log n)^{2/3}}$

(1998) 130 digits/month

⇩

400 digits/ 10^{10} years

Polynomial in # of digits

Shors algorithm: $\mathcal{O}[(\log n)^3]$

130 digits/mo. ⇨ 400 digits/3 yrs if Quantum

Introduction and Overview (Preskills Notes)

Efficient Factoring

Factoring $n = p \times q$ ➔ RSA encryption

large integer (n) — large prime numbers (p, q)

- easy to verify solution $\log n$ steps
- very hard to solve $O[n]$ steps

Exponential in # of digits

$\boxed{\text{QFT} \Rightarrow \text{Solvable}}$

Preskill Ch. 1, p. 5-6 $T \propto e^{1.9(\log n)^{1/3}} e^{(\log \log n)^{2/3}}$

(1998) 130 digits/month

400 digits/ 10^{10} years

Polynomial in # of digits

Shors algorithm: $O[(\log n)^3]$

130 digits/mo. ➔ 400 digits/3 yrs if Quantum

Quantum Complexity

Benioff, Feynman ➔ Simulating QM is hard

Simulating Physics with computers (1982)

qubit $|1\rangle$, $|0\rangle$ $\qquad |\psi\rangle = a|0\rangle + b|1\rangle$

N qubits ➔ $\underbrace{|0110101\ldots010\rangle}$ $= |x\rangle \in \mathcal{E}$

N bit integer = X : logical basis state

2^N - dimensional Hilbert Space

General State: $\boxed{|\psi\rangle = \sum_{x=0}^{2^N-1} a_x |x\rangle}$

Introduction and Overview (Preskills Notes)

Quantum Complexity

Benioff, Feynman ⇒ **Simulating QM is hard**

Simulating Physics with computers (1982)

qubit

$|1\rangle$

$|0\rangle$

$|\psi\rangle = a|0\rangle + b|1\rangle$

N qubits ⇒ $\underbrace{|01101011\ldots010\rangle}_{} = |x\rangle \in \mathcal{E}$

N bit integer = X : logical basis state

2^N - dimensional Hilbert Space

General State: $$\boxed{|\psi\rangle = \sum_{x=0}^{2^N-1} a_x |x\rangle}$$

Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981

1. INTRODUCTION

On the program it says this is a keynote speech—and I don't know what a keynote speech is. I do not intend in any way to suggest what should be in this meeting as a keynote of the subjects or anything like that. I have my own things to say and to talk about and there's no implication that anybody needs to talk about the same thing or anything like it. So what I want to talk about is what Mike Dertouzos suggested that nobody would talk about. I want to talk about the problem of simulating physics with computers and I mean that in a specific way which I am going to explain. The reason for doing this is something that I learned about from Ed Fredkin, and my entire interest in the subject has been inspired by him. It has to do with learning something about the possibilities of computers, and also something about possibilities in physics. If we suppose that we know all the physical laws perfectly, of course we don't have to pay any attention to computers. It's interesting anyway to entertain oneself with the idea that we've got something to learn about physical laws; and if I take a relaxed view here (after all I'm here and not at home) I'll admit that we don't understand everything.

The first question is, What kind of computer are we going to use to simulate physics? Computer theory has been developed to a point where it realizes that it doesn't make any difference; when you get to a *universal computer*, it doesn't matter how it's manufactured, how it's actually made. Therefore my question is, Can physics be simulated by a universal computer? I would like to have the elements of this computer *locally interconnected*, and therefore sort of think about cellular automata as an example (but I don't want to force it). But I do want something involved with the

Introduction and Overview (Preskills Notes)

Quantum Complexity

Benioff, Feynman → **Simulating QM is hard**

Simulating Physics with computers (1982)

qubit $|1\rangle$, $|0\rangle$ $\quad |\psi\rangle = a|0\rangle + b|1\rangle$

N qubits → $\underbrace{|0110101\ldots010\rangle}_{}= |x\rangle \in \mathcal{E}$

N bit integer = X : logical basis state

2^N - dimensional Hilbert Space

General State:

$$\boxed{|\psi\rangle = \sum_{x=0}^{2^N-1} a_x |x\rangle}$$

Quantum Computation

Computation is a map

$$|\psi_{in}\rangle \rightarrow U|\psi_{in}\rangle = |\psi_{out}\rangle$$

input "program" output

access via measurement

Schrödinger Evolution

$$i\hbar \frac{dU}{dt} = HU$$

given enough memory & time we can find U

Introduction and Overview (Preskills Notes)

Quantum Computation

Computation is a map

$$|\psi_{in}\rangle \to U|\psi_{in}\rangle = |\psi_{out}\rangle$$

input — "program" — output

access via measurement

Schrödinger Evolution

$$i\hbar \frac{dU}{dt} = HU$$

given enough memory & time we can find U

Quantum Computation

* A classical computer can simulate a QC
* Notion of computability unchanged

Simulation is <u>hard</u> :

N bits $\quad 2^N$ prob. amp's

$N = 100 \to 2^{100} \sim 10^{30}$ p. a's

$N = 300 \to 2^{300} \sim 10^{90}$ p. a's

10^{90} >> # of particles in the visible universe

Jeff Kimble: Hilbert Space is a mighty big place