Begin
8-27-2024

Introduction and Overview (Preskills Notes)

Physics of Information: John von Neumann
Alan Turing

Notions: What is a computation ?
What is computable

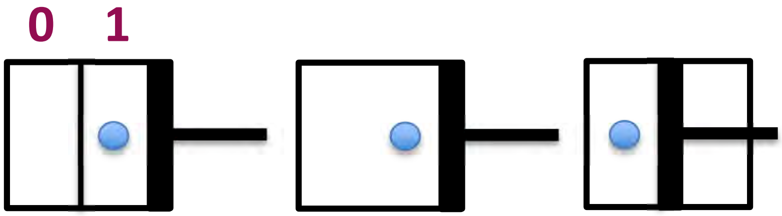
Formulation of Computer Science that is Device Independent

1937 Turing Machine:

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

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)

John von Neumann
Alan Turing

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.

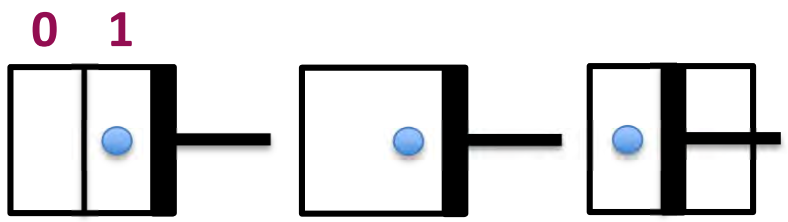
At each step the head reads the symbol in the cell. Then, based on the symbol and the TM's present state, the machine writes a symbol in the cell, and moves the head one step to the left or the right, or halts the computation.

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 ?

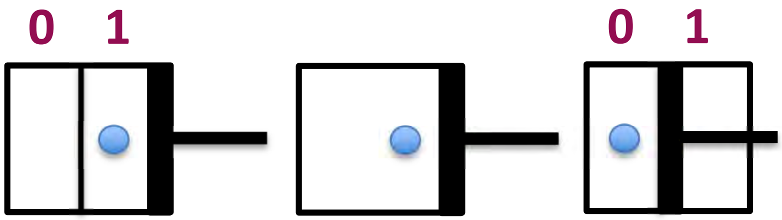
Reversible Computation !

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

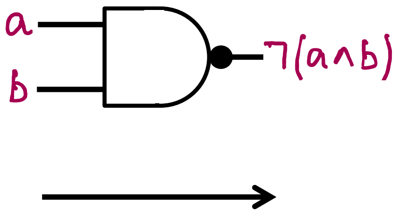
$\sim 3 \times 10^{-21} J \sim 0.02 eV$

Is there a way around it ?

Reversible Computation !

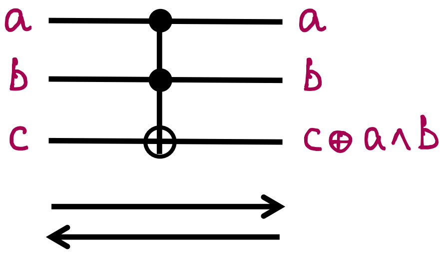
But we need a different gate set !

NAND Gate:



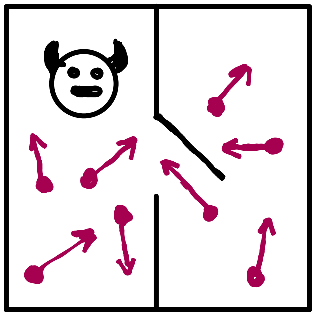
irreversible

Toffoli Gate:



reversible

Maxwells Demon:



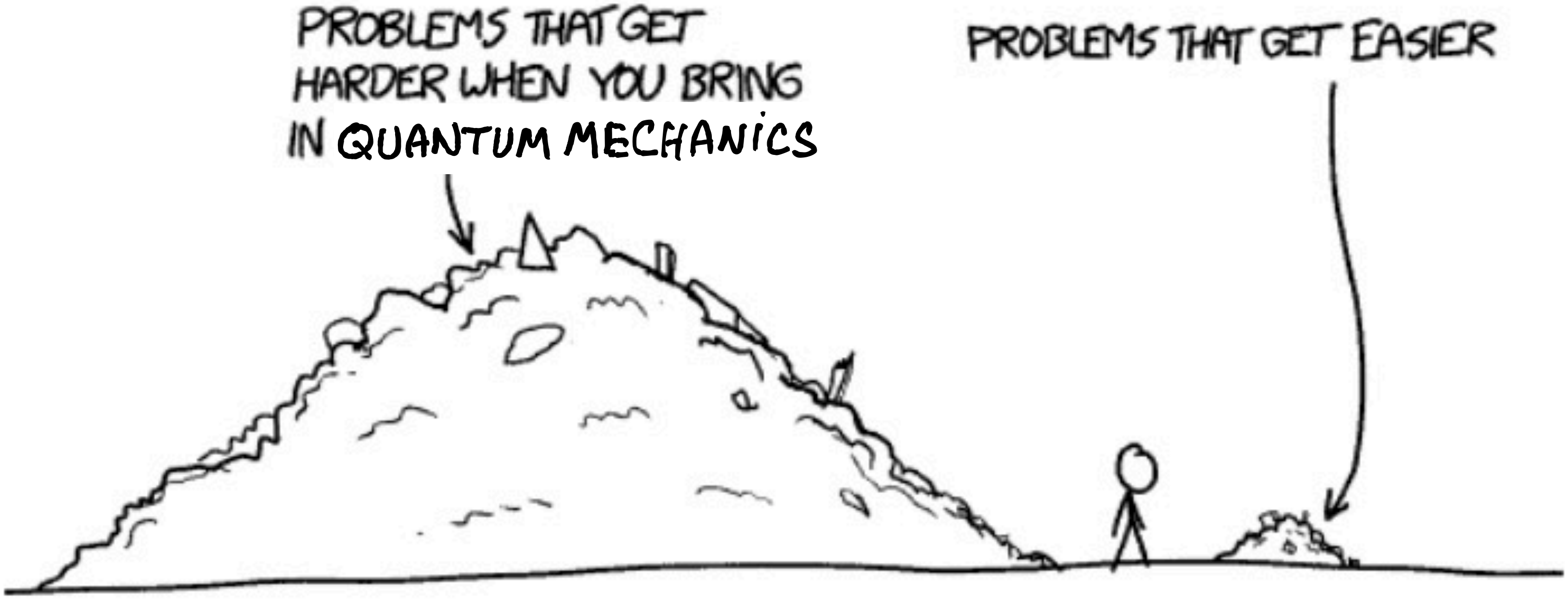
Information is Physical !

Quantum Information

Carl Caves: Quantum States are states of knowledge

Physics is Information !

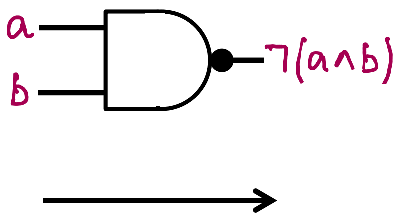
Introduction and Overview (Preskills Notes)



Source: xkcd.com

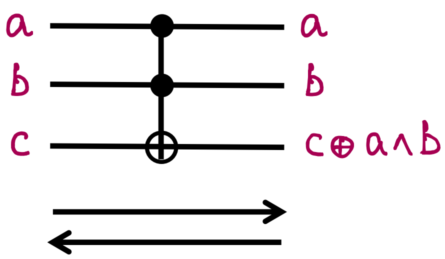
Introduction and Overview (Preskills Notes)

NAND Gate:



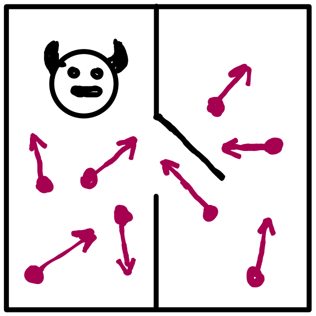
irreversible

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 quantum system if initially unknown } Cannot Copy
No cloning theorem

Entanglement:

Non-local correlations

pure state, entangled

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

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

mixed state,
not entangled

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 ↑ ↑ large prime numbers

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

↓

Exponential in # of digits

QFT → Solvable

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

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 "	$\mathcal{O}[N2^N]$	**"**
QFT on "	$\mathcal{O}[N \mathrm{Log} N]$	**"**

Efficient Factoring

Factoring $n = p \times q$ ➡ **RSA encryption**

large integer ↑ n; ↑ p, q large prime numbers

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

⬇

Exponential in # of digits

QFT ➡ Solvable

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

(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 "	$\mathcal{O}[N2^N]$	"
QFT on "	$\mathcal{O}[N \, \mathrm{Log} N]$	"

Efficient Factoring

Factoring $n = p \times q$ ⇒ **RSA encryption**

large integer → n large prime numbers → p, q

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

⇓

Exponential in # of digits

QFT ⇒ Solvable

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

(1998) 130 digits/month

⇓

400 digits/ 10^{10} years

Shors algorithm: $\mathcal{O}[(\mathrm{Log}\, n)^3]$ ← Polynomial in # of digits

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; p, q ← large prime numbers

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

⇩

Exponential in # of digits

QFT ⇨ Solvable

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

(1998) 130 digits/month

⇩

400 digits/ 10^{10} years

Polynomial in # of digits

Shors algorithm: $\mathcal{O}[(\text{Log}\, n)^3]$ ←

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

End 8-27-2024