Quantum Computing

The Laws of Nature,
or
How everything works

Computers and how they work

Professor Andrew M. Steane
Oxford University

Popular Mechanics magazine, March 1949:

"Where a calculator on the Eniac is equipped with 18,000 vacuum tubes and weighs 30 tons, it is possible that the computer of the future may have only 1,000 vacuum tubes and weigh only 1.5 tons."

Summary

1. Quantum *entanglement* shows that the physical world is not fully separable into component parts

2. Quantum computing offers a tremendous speed-up on certain specialised mathematical problems

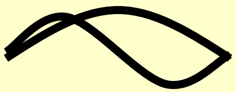
3. A brief impression of how it works

PART 1:

QUANTUM ENTANGLEMENT

Quantum "Superposition"

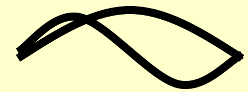
Examples of objects that are "two things at once"

1. an oscillating guitar string 

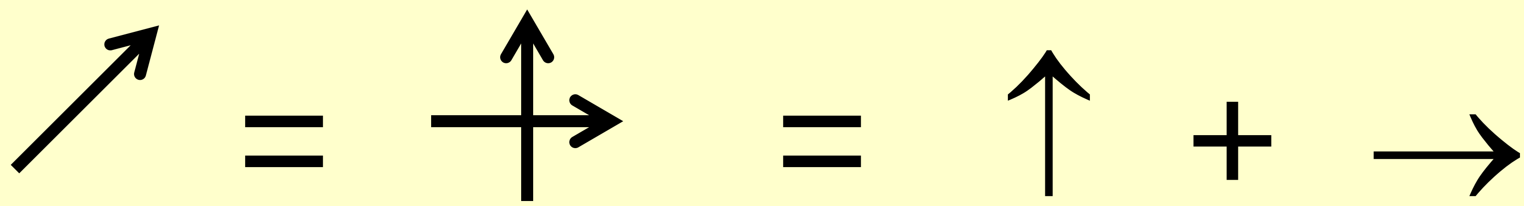
Quantum superposition

Examples of objects that are “two things at once”

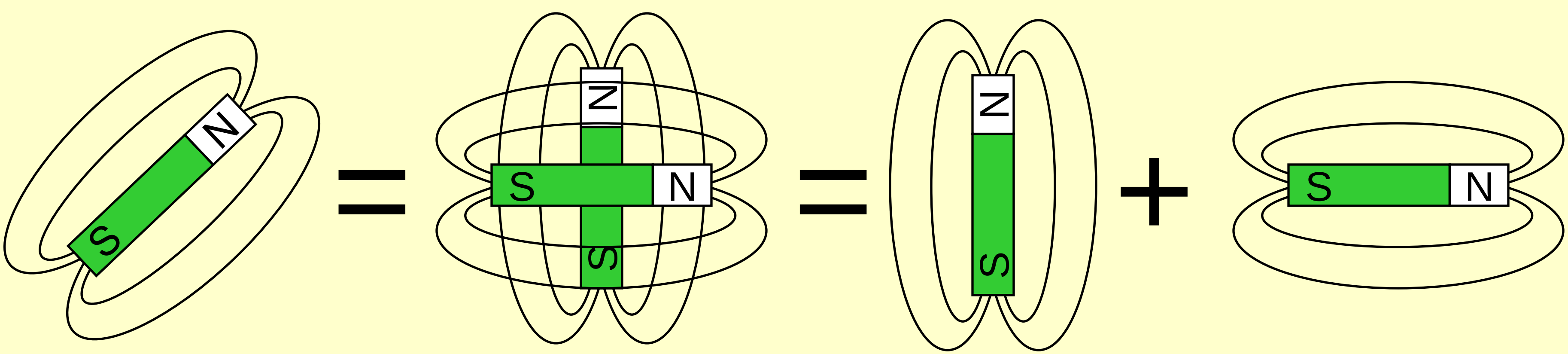
1. an oscillating guitar string



2. a step up a hill:

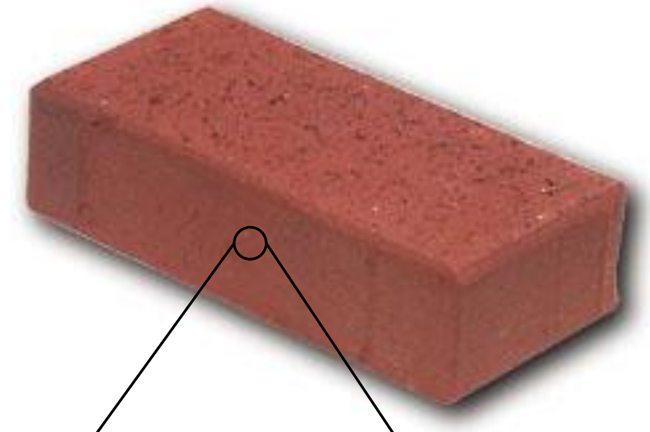


3. A small magnet

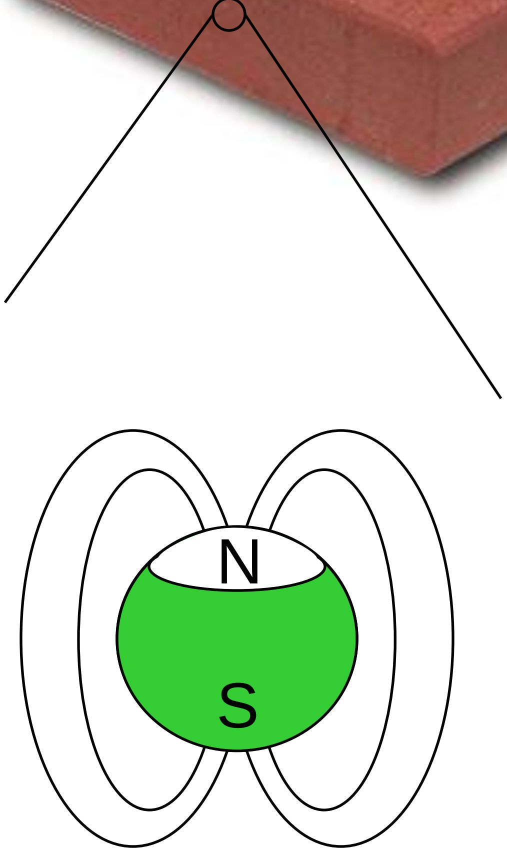


Atoms

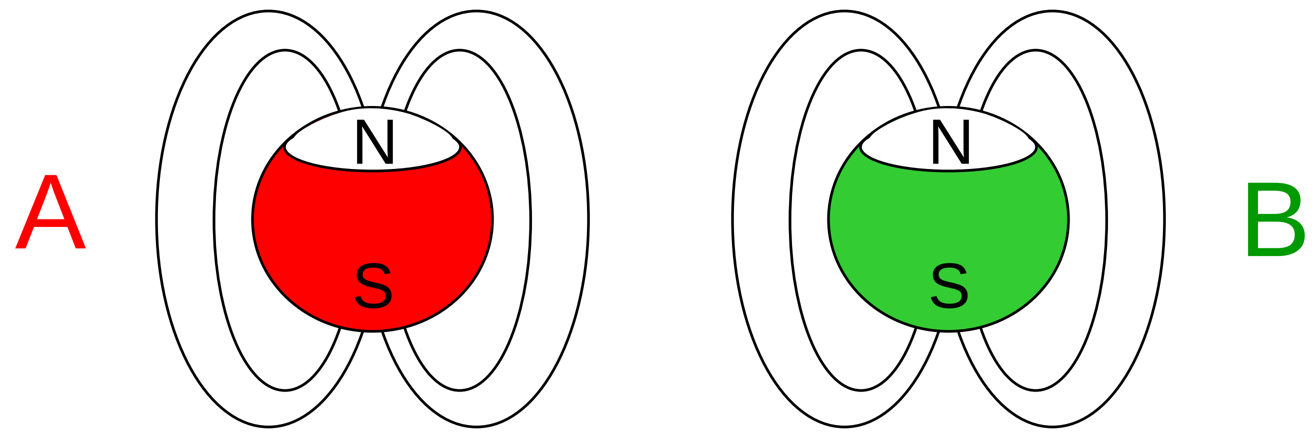
Things (for example, a brick) are made of atoms.

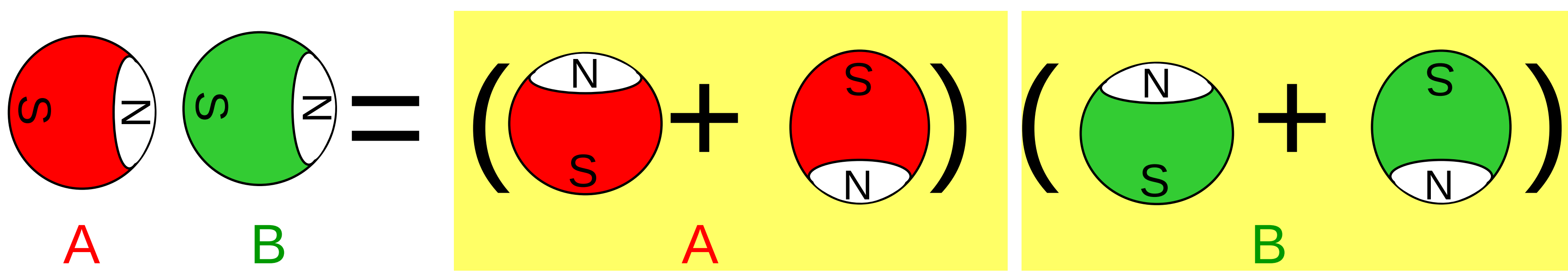


Atoms are small magnets !



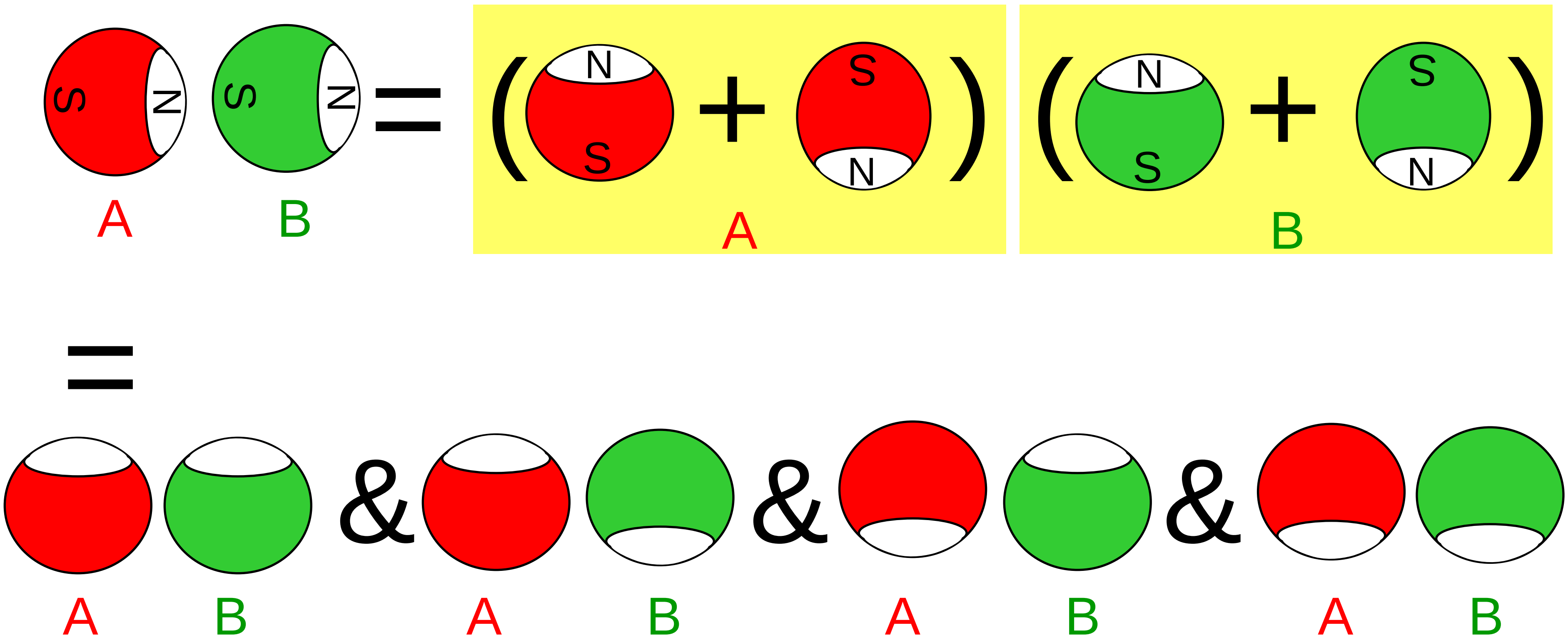
Quantum superposition with atoms





$$|\rightarrow\rangle|\rightarrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle + |\downarrow\rangle\right)\frac{1}{\sqrt{2}}\left(|\uparrow\rangle + |\downarrow\rangle\right)$$

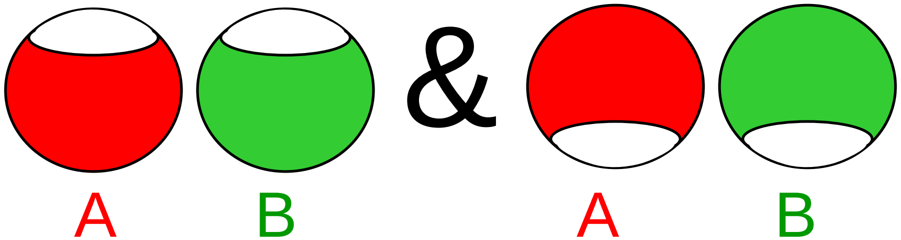
Two atoms



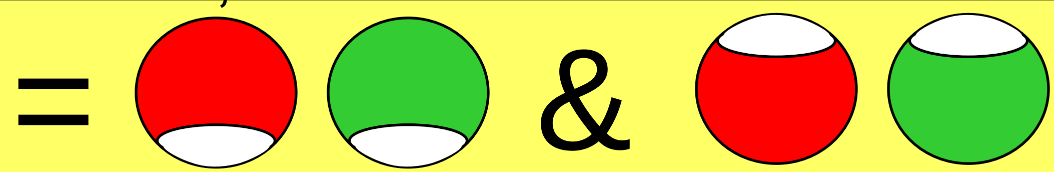
$$\frac{1}{2}\left(|\uparrow\rangle|\uparrow\rangle + |\uparrow\rangle|\downarrow\rangle + |\downarrow\rangle|\uparrow\rangle + |\downarrow\rangle|\downarrow\rangle\right)$$

An important property of *entanglement*

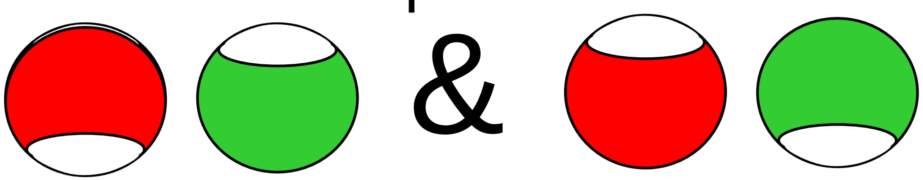
It is possible to place two atoms in the "entangled" state:



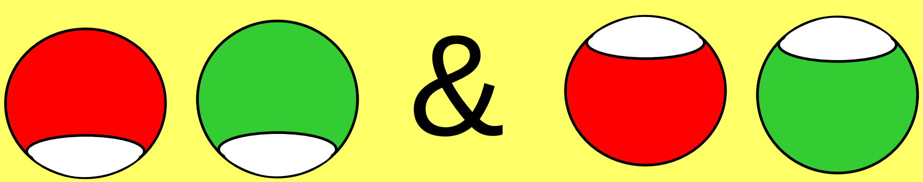
The order of writing doesn't matter, so



Turn atom A upside down:

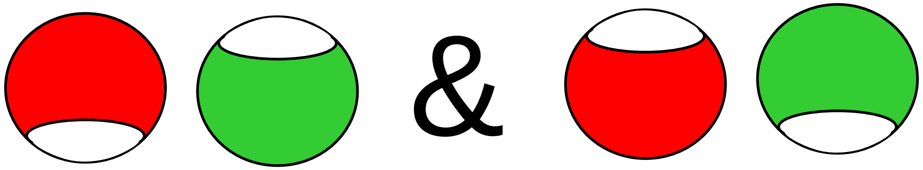


Now turn atom B upside down:



But this is exactly what we started with!!!

The unity of the entangled state

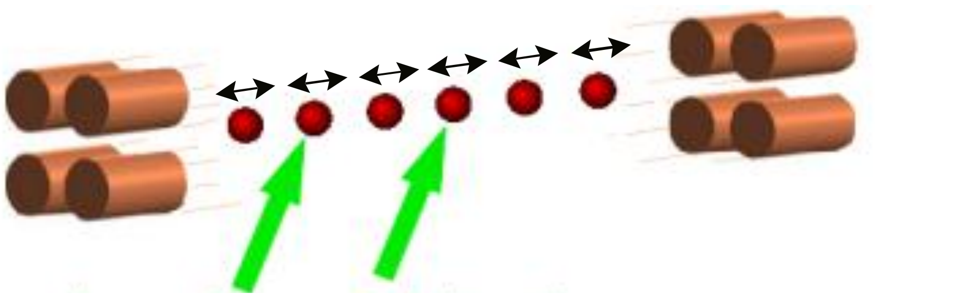


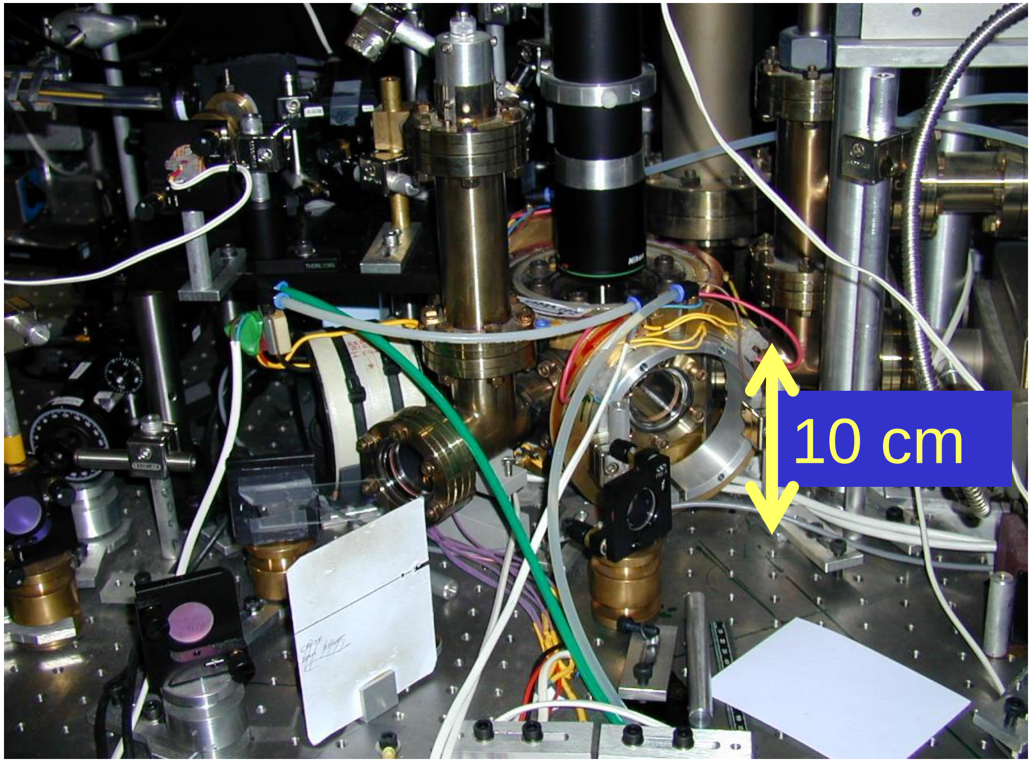
After turning one atom upside down, if I want to get back to where I started I can now turn **either** of the two atoms.

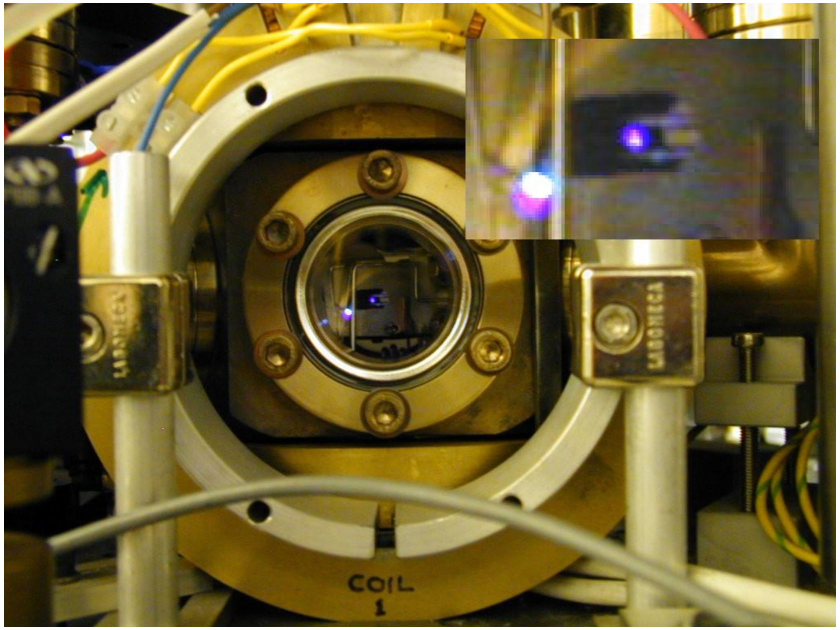
It is as if I only have ONE object, even though it is made of two parts which can be in separate places.

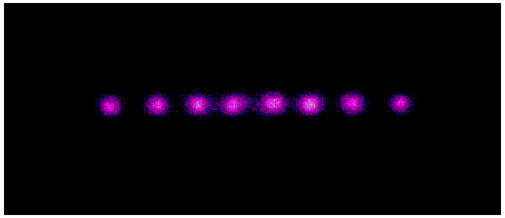
The Oxford Atom Trap Quantum Computer

A string of calcium atoms held in a vacuum chamber and manipulated by laser beams:









8 atoms in the trap!

Part 2:

Information and Physics

The same information expressed in different ways

"The quantum computer is very interesting."

"L'ordinateur quantique est très intéressant."

a→97, b→98, c→99:

116 104 101 32 113 117 97 110 116 117 109 ...

1110100 1101000 1100101 100000 1110001 ...

Compare with other basic concepts in physics

c.f. Energy, momentum

kinetic energy example:

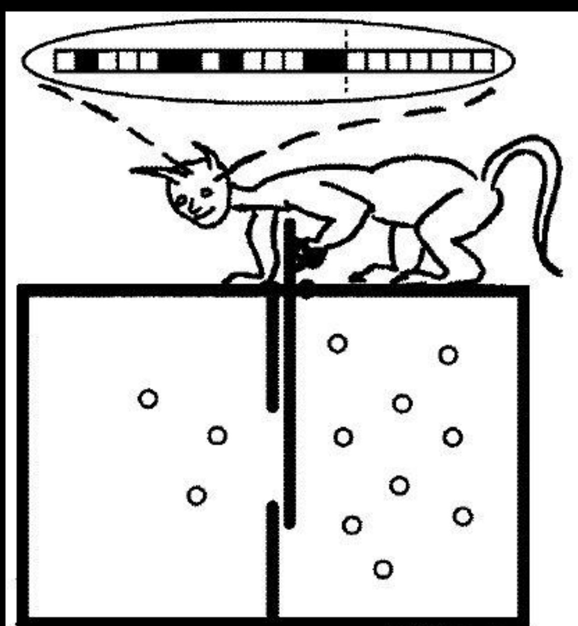
Proton at CERN ←→ a rolling marble

Information is another basic physical property whose behaviour is described by the laws of Nature.

Examples of the physics of information

1. "Speed of light"
   = speed of information

Information cannot travel faster than 299,792,458 metres per second



2. Thermal physics
… information and entropy

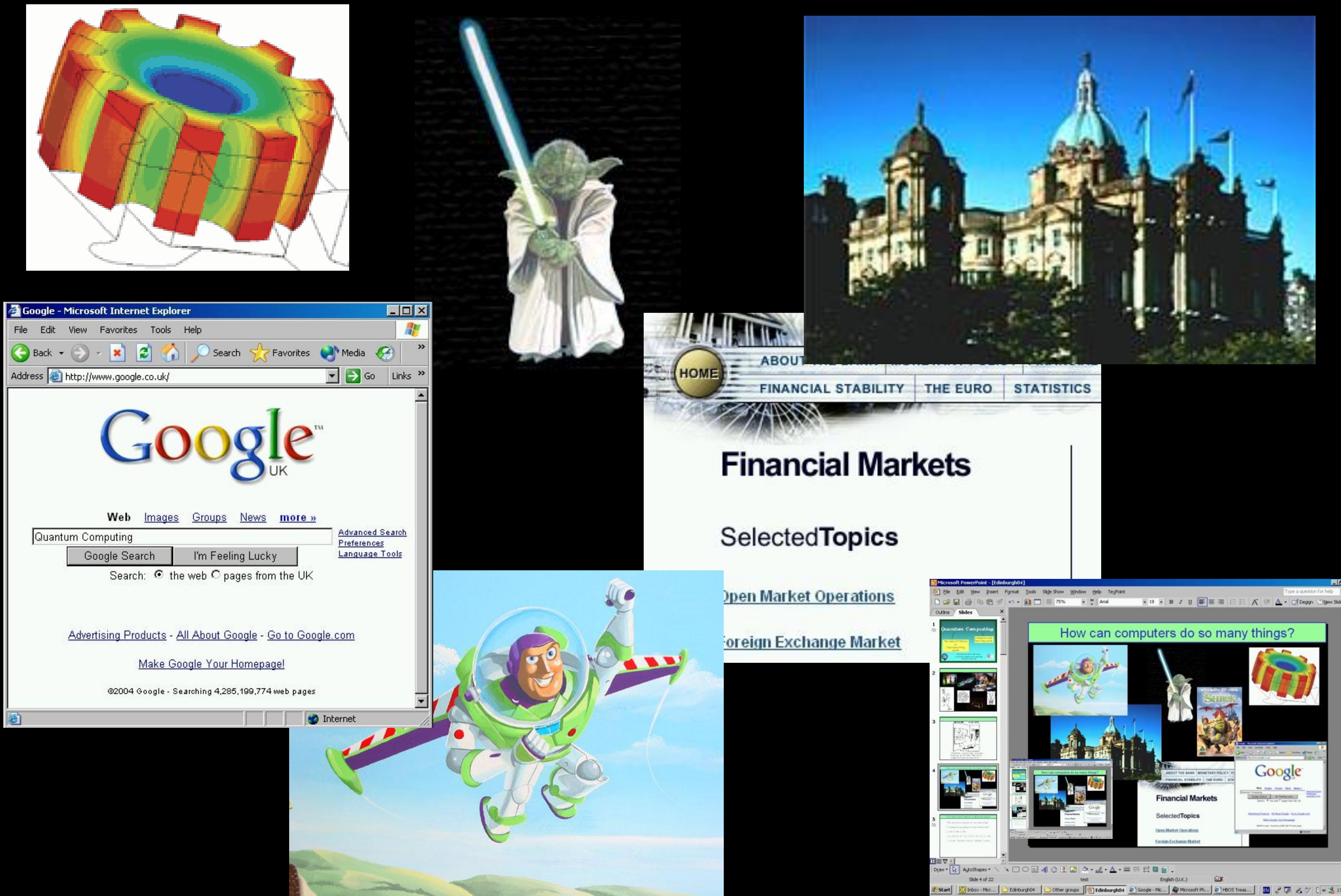
Classical computer science: 2 main ideas

- All computers are alike (Turing 1920s)

→ *Universal* machine:
One machine can simulate another

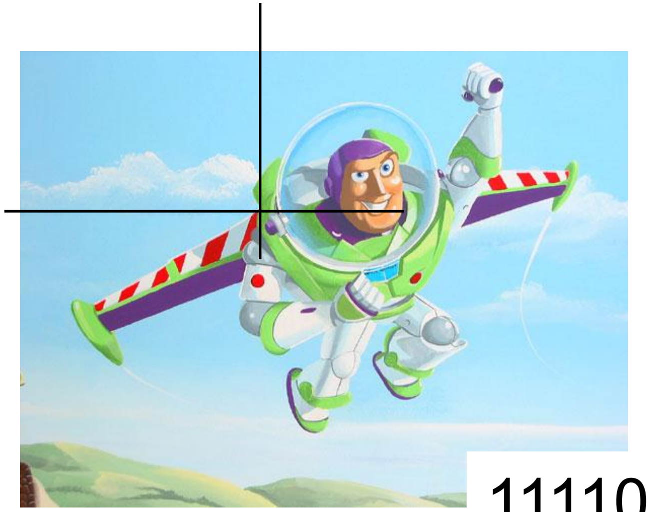
- Speed of an algorithm is measured by how the number of steps scales with the input size ("polynomial" verses "exponential")

Flexibility of information processing



The flexibility of information processing

10100 1000 101 0 1 111 10101 1 1110 10100 10101 …



1111000 10000010 1 111001 10000010 1 …

Quantum computers are **fast** at some calculations

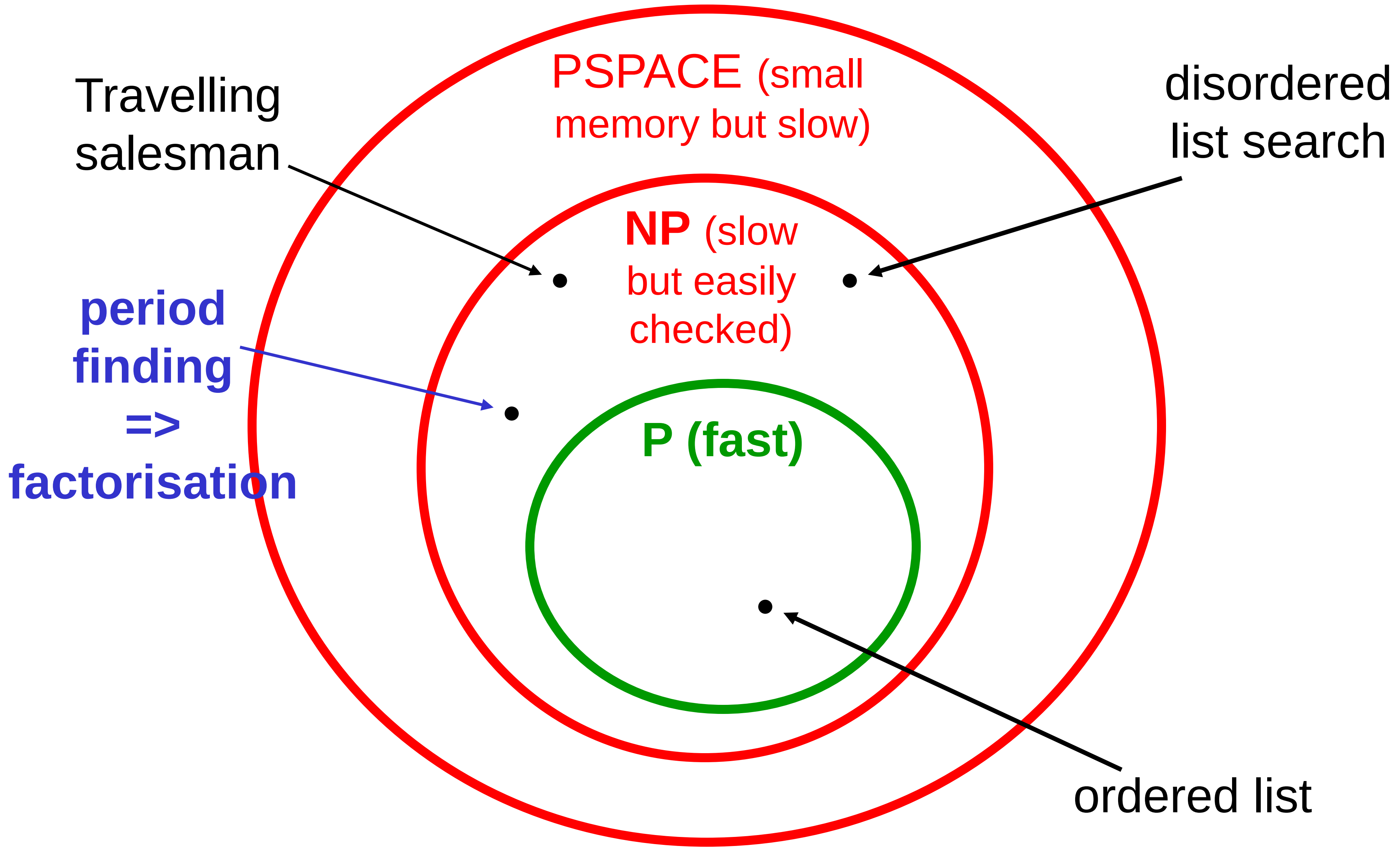
24 17 6 3 24 17 6 3 24 17 6 3 24 17 6 3 24 17 6 3

Period finding: Given $f(x)$ such that $f(x+ n\,p) = f(x)$
(i.e. periodic with period p), find the period p.

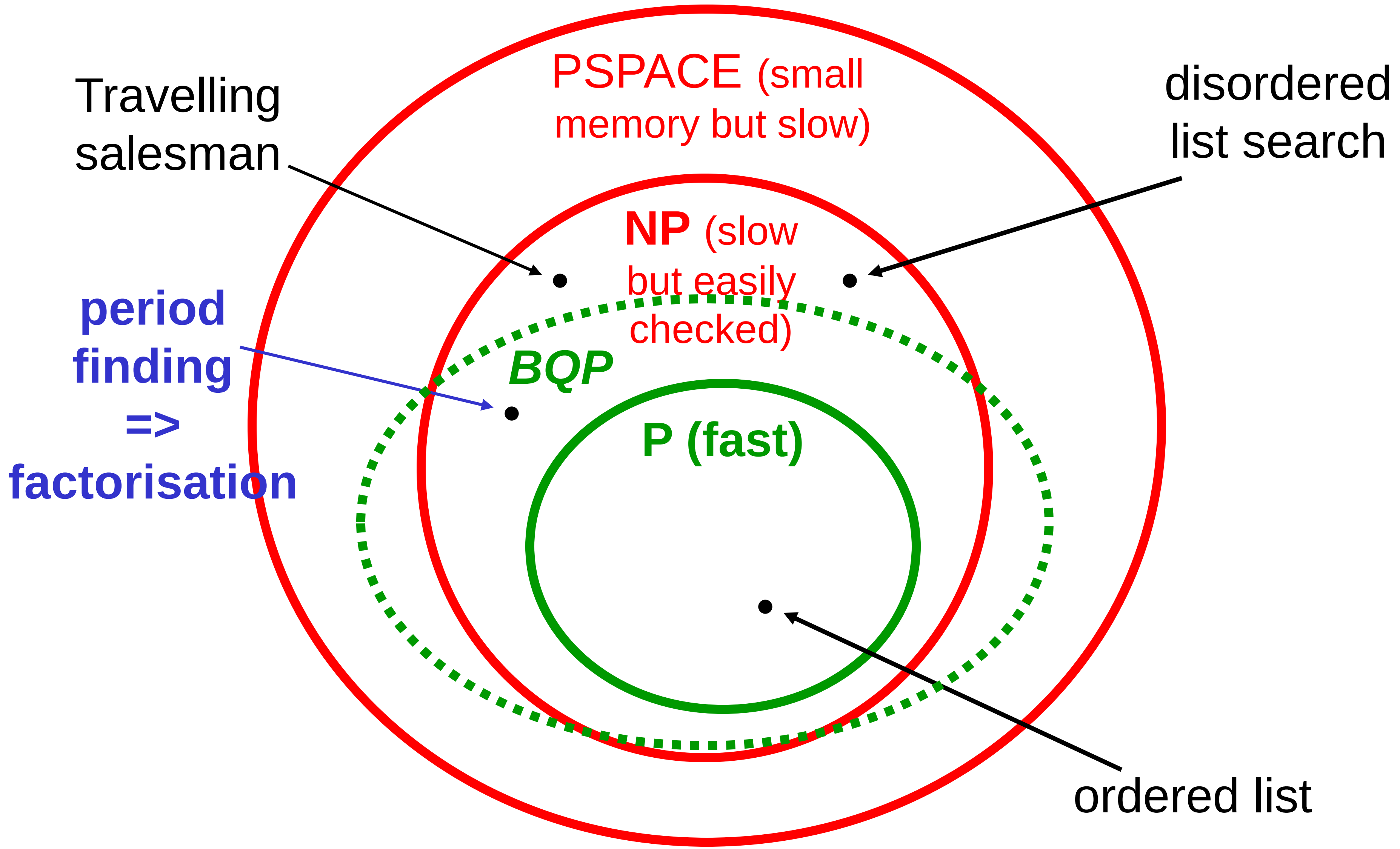
24 17 6 3 18 9 2 65 72 45 7 8 12 22 28 36 47 55 27 51 64
1 81 98 32 41 74 5 19 23 33 25 37 52 63 83 92 16 31 43
87 72 73 91 31 14 11 4 38 1 20 3 13 10 15 25 18 26 30 29
34 42 35 37 39 61 71 46 90 48 49 53 56 86 62 21 27 34 24
17 6 3 18 9 2 65 72 45 7 8 12 22 28 36 47 55 27 51 64 1
81 98 32 4 1 74 5 19 23 33 25 37 52 63 83 92 16 31 43 87
72 73 91 31 14 11 4 38 1 20 3 13 10 15 25 18 26 30 29 34
42 35 37 39 61 71 46 90 48 49 53 56 86 62 21 27 34 24 17
6 3 18 9 2 65 72 45 7 8 12 22 28 36 47 55 27 51 64 1 81
98 32 41 74 5 19 23 33 25 37 52 63 83 92 16 31 43 87 72
73 91 31 14 11 4 38 1 20 3 13 10 15 25 18 26 30 29 34 42
35 37 39 61 71 46 90 48 49 53 56 86 62 21 27 34 24 17 6
3 18 9 2 65 72 45 7 8 12 22 28 36 47 55 27 51 64 1 81 98
32 41 74 5 19 23 33 25 37 52 63 83 92 16 31 43 87 72 73
91 31 14 11 4 38 1 20 3 13 10 15 25 18 26 30 29 34 42 35

Repeats every 78 numbers

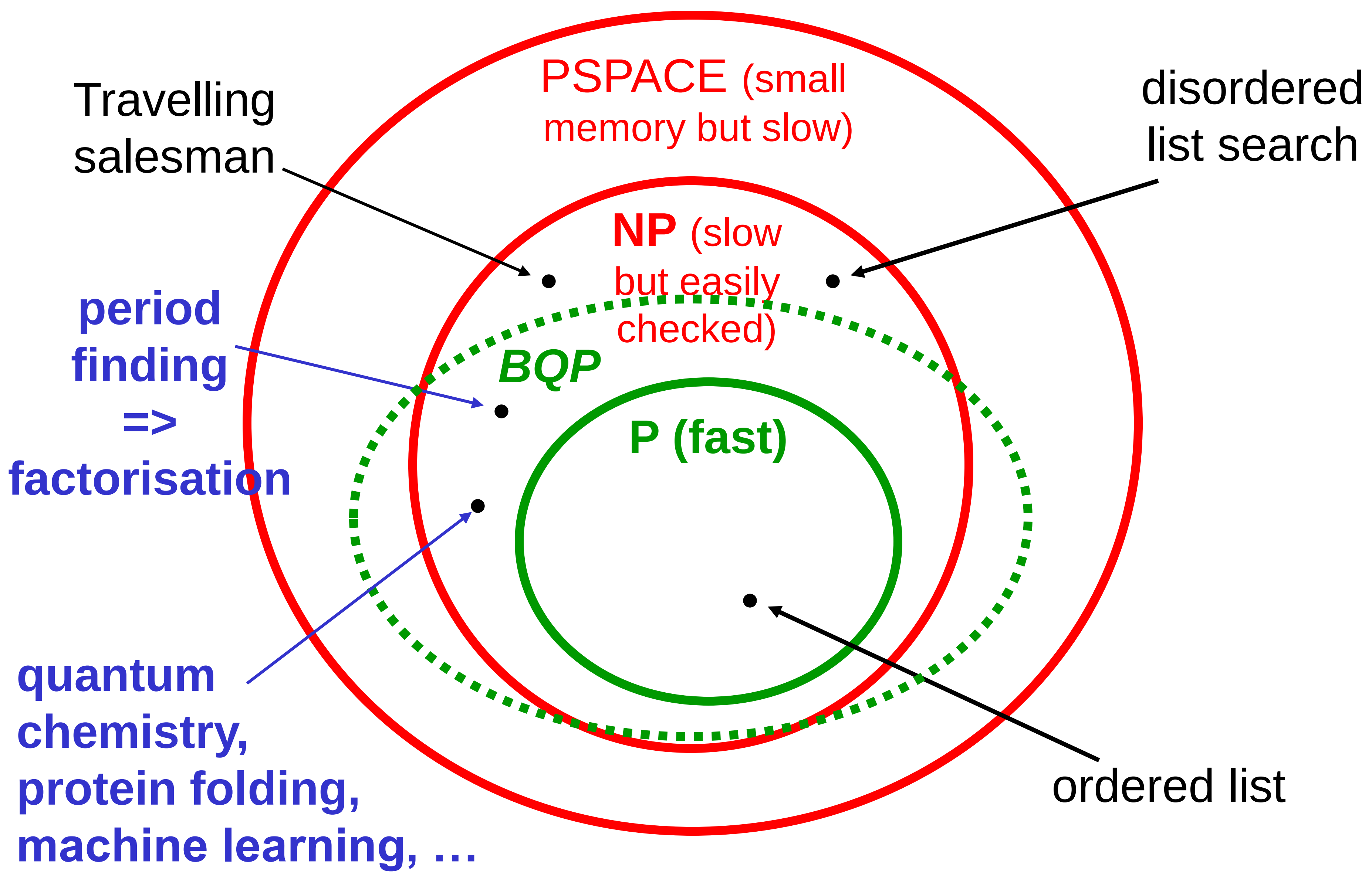
“Complexity classes”



“BQP”=Bounded error, quantum, polynomial time



“BQP”=Bounded error, quantum, polynomial time



Quantum computing cannot calculate anything that could not in principle be calculated by an ordinary computer that runs for long enough.

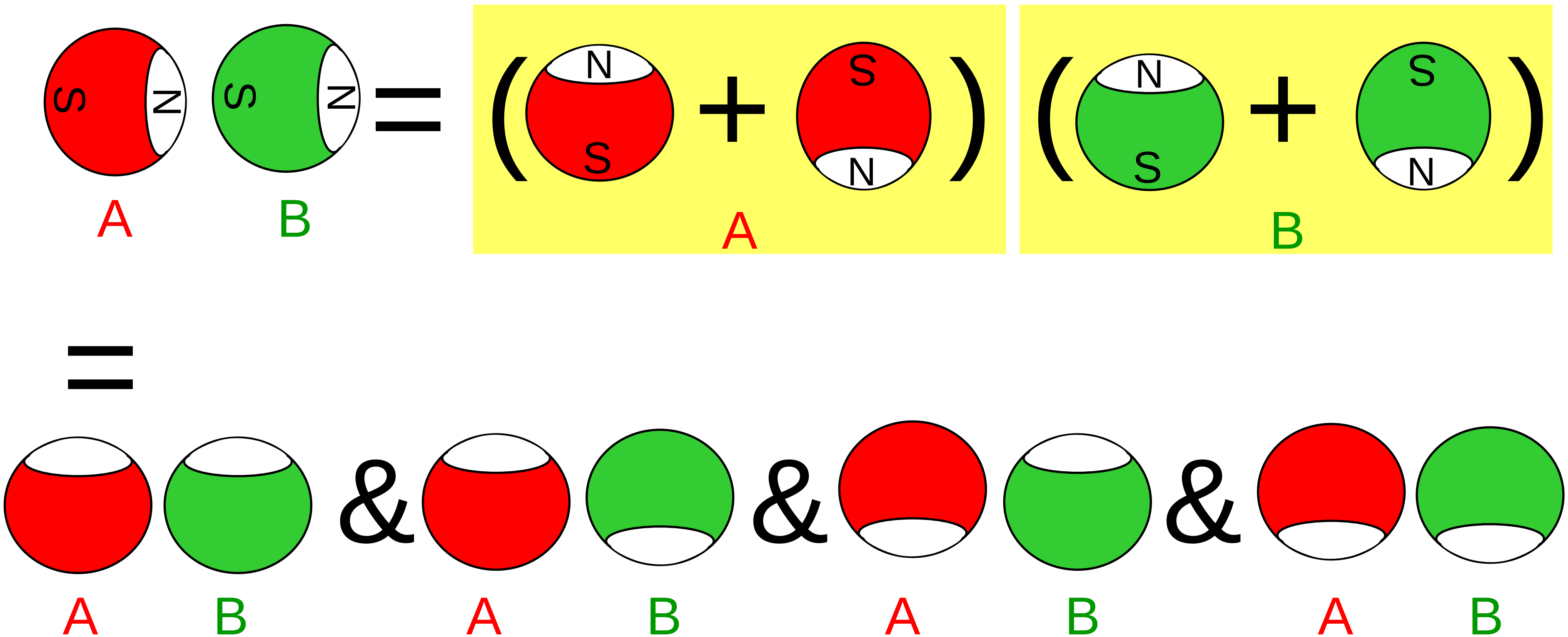
However, “long enough” might be millions of years!

That is to say, there exist significant tasks for which a traditional computer would require millions of years (or millions of processors), whereas a quantum computer would complete the calculation in seconds or hours.

PART 3:

HOW A QUANTUM COMPUTER WORKS

Two atoms

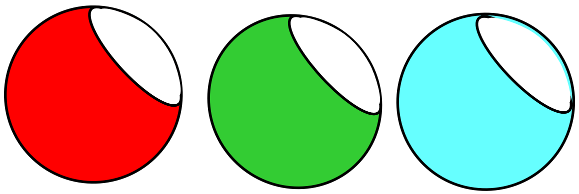


1 1	1 0	0 1	0 0

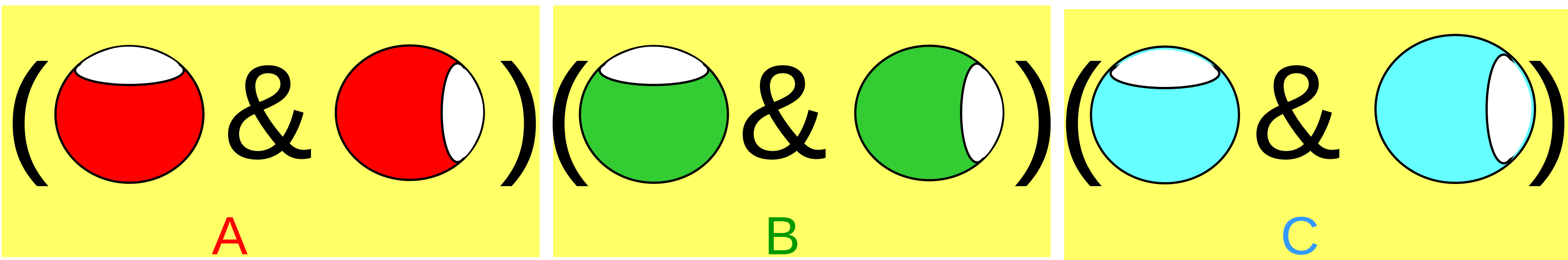
=

3	2	1	0

More atoms



=



=

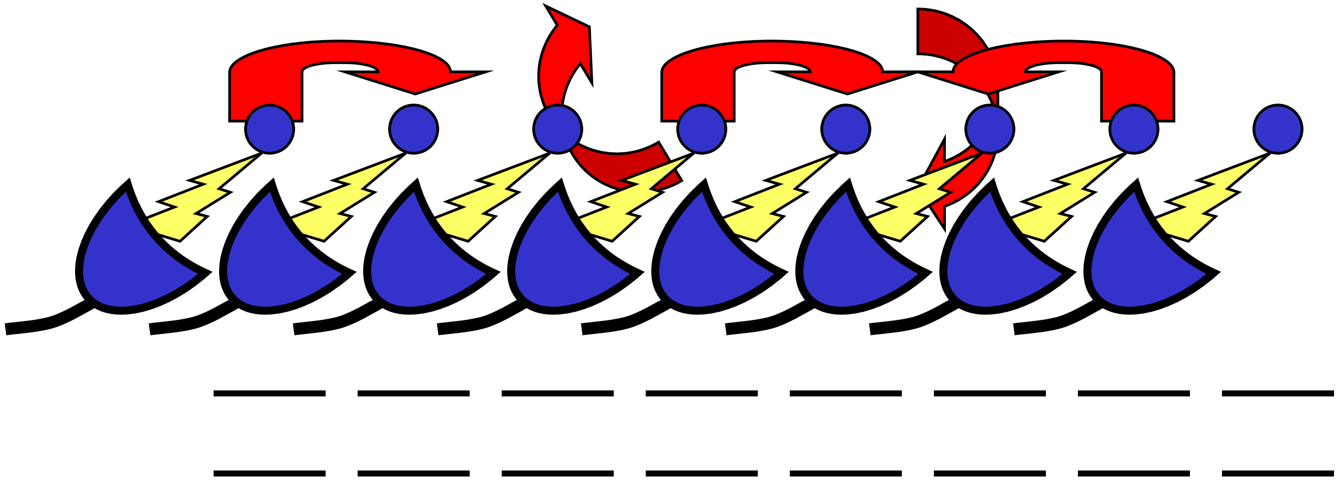
111 & 110 & 101 & 100 & 011 & 010 & 001 & 000

so 3 atoms can keep track of 8 numbers
… 4 atoms can keep track of 16 numbers
… … 23 atoms can compute 10 million numbers
… … 100 atoms can compute 100 billion billion Gbytes !

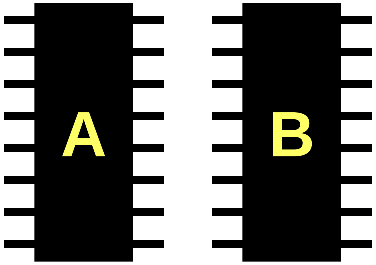
Universal quantum computer (Deutsch 1985)

1. Well-behaved and controllable set of 2-state systems (e.g. atoms) = set of *qubits* = quantum register
2. Prepare initial state, e.g. all in ground state
3. Single-bit gate = general rotation of any one qubit
4. Two-bit ‘logic gate’ (for example, controlled-rotation) between chosen neighbouring pairs
5. Measure final state

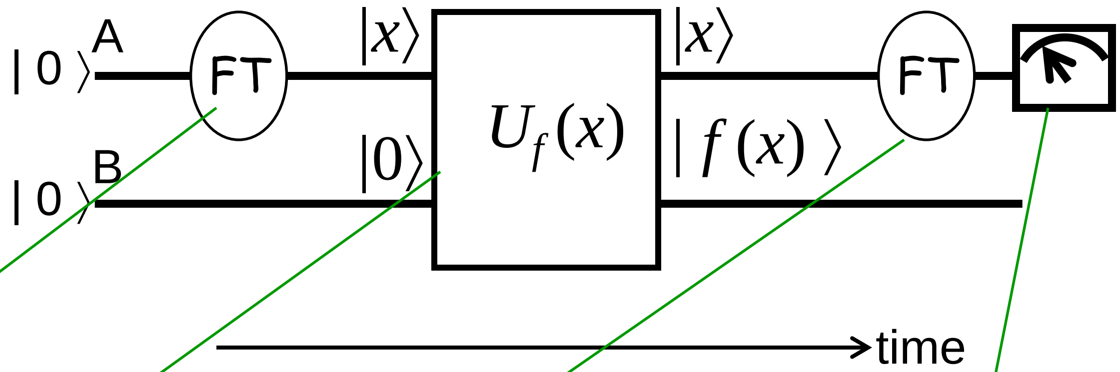
Sufficient to simulate ANY quantum evolution !



Entanglement and quantum parallelism



The computer:
2 registers, n qubits each



Network diagram

Fourier transform network: $$|0\rangle|0\rangle \rightarrow \sum_{x=0}^{2^n-1} |x\rangle|0\rangle$$

Effect of U: $$\sum_{x=0}^{2^n-1} |x\rangle|0\rangle \rightarrow \sum_{x=0}^{2^n-1} |x\rangle|f(x)\rangle$$

"Quantum Parallelism"

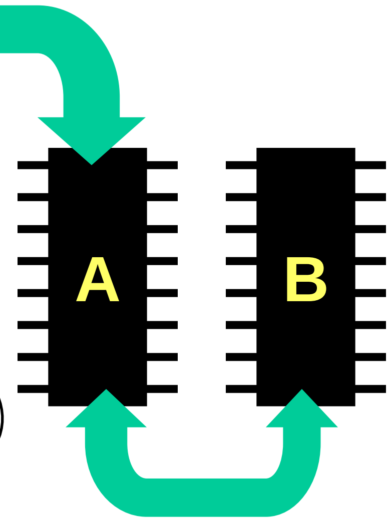
The periodicity of $f(x)$ in register B is now reflected in register A by entanglement

Second Fourier transform: reorganise register A to move a random offset into the overall phase of the state → makes the (inverse) period appear in measured result.

A quantum algorithm: e.g. period-finding

14 17 6 3 18 9 2 6 21 27 34 45 7 8 12 22 28 36 47
98 5 19 23 33 25 37 52 63 83 92 16 32 43 87 72 73
91 31 24 11 4 38 51 14 17 6 3 18 9 2 6 21 27 …

Put into A the numbers x=0,1,2,3,4 … all at once



A,B=
0, 14
& 1, 17
& 2, 6
& 3, 3
& 4, 18
…

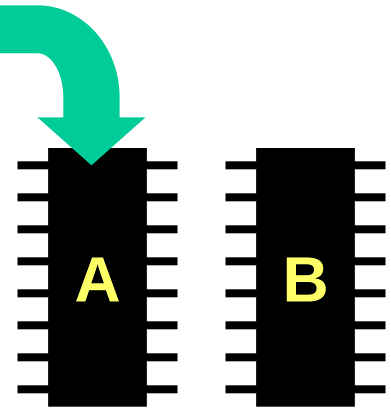
In B calculate the sequence f(x)=14,17,6,3,18, … all at once

Next, observe ("measure") B.

e.g. suppose number 17 is found in B. Suddenly, by entanglement, the only numbers left in A are 1, 43, 85, ...

The Quantum Computer: period-finding

Now Fourier transform A:
N.B. this quantum FFT algorithm is EFFICIENT



A,B=

& 1, 17
& 43, 17
& 85, 17
& 127,17
...

Finally, observe ("measure") A.

The number in A gives the period r of the Fourier series, and the period of the original function is $p = N / r$.

Feasibility?

To factorize a 200-digit (600 bit) number
the algorithm needs approximately

$2n \ = \ 1000$ qubits,

$n^3 \ = \ 10^9$ operations

Therefore each operation has to have precision about
1 part in 10^9 !!

This looks impossible.

Controlling errors

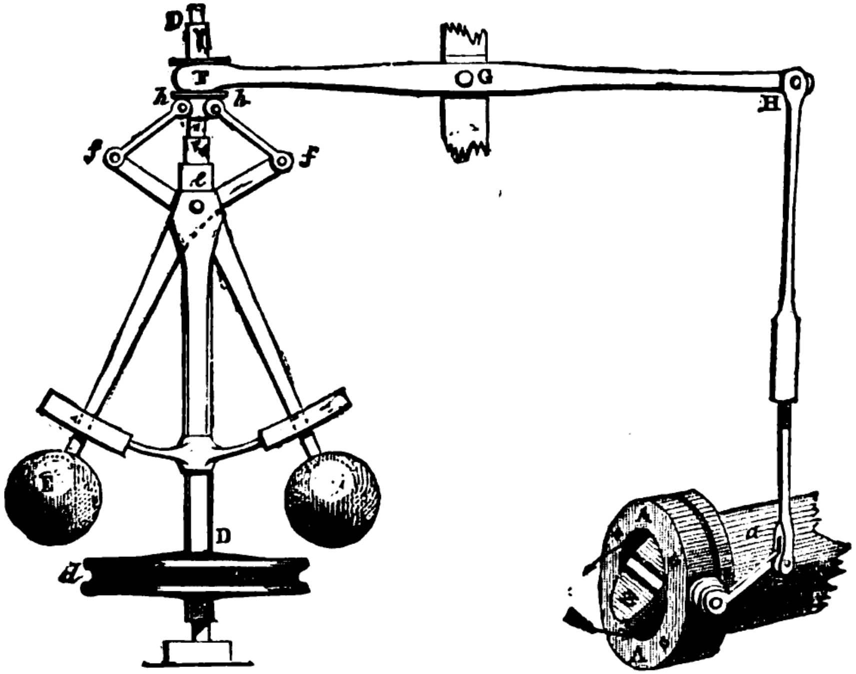
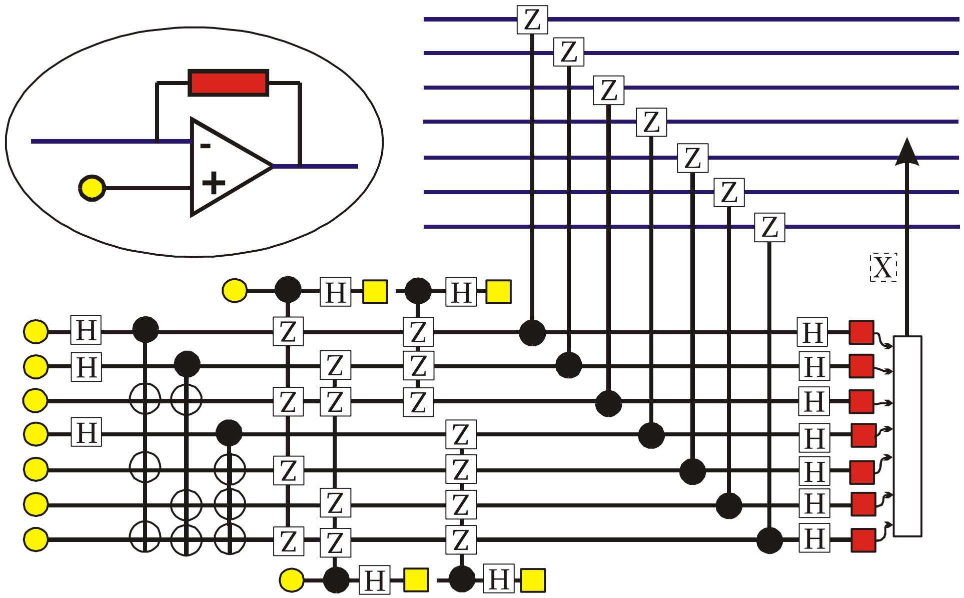


FIG. 4.—*Governor and Throttle-Valve.*

Stabilization requires **detection** and **feedback**,

BUT you can't observe a quantum state without disturbing it!

Quantum Error Correction



quantum network for preparing error-correcting code word, and getting error syndrome

- Quantum information is now distributed in a subtle way in multi-qubit entangled states
- With these states we can find global check measurements which observe (and disturb) the errors *without* observing the stored quantum information.

Most financial and diplomatic transactions done in the world today derive their security from coding methods which a quantum computer can break … but you can still resort to very long keys.

Fortunately, quantum mechanics also provides new methods that allow truly unbreakable codes.

However, the most interesting scientific and commercial application of quantum computers is in quantum chemistry and biochemistry … possible impact on pharmaceuticals etc.

The other thing I learn from all this is how subtle and wonderful the world is.