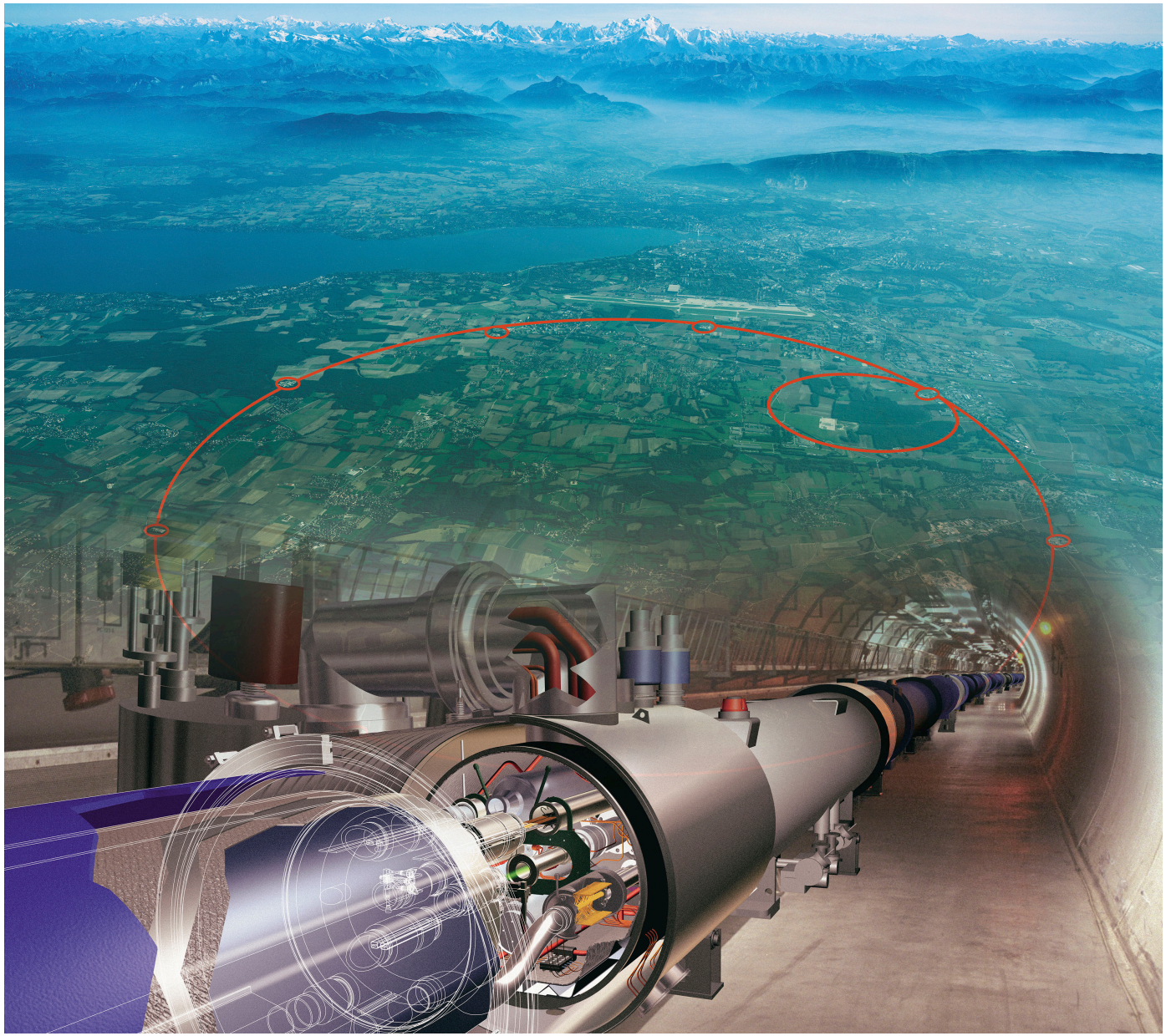
QUANTUM COMPUTING

A ~~Very~~ Gentle ish Glimpse into a ~~Possible~~ Likely Future

How it isn't what all those pop articles say it is

Nick Radcliffe
Stochastic Solutions Limited
& University of Edinburgh, Mathematics

The Higgs Boson & LHC



Alice laughed. 'There's no use trying,' she said. 'One can't believe impossible things.'

I daresay you haven't had much practice,' said the Queen. 'When I was your age, I always did it for half-an-hour a day. Why, sometimes I've believed as many as six impossible things before breakfast.'

Through the Looking Glass
— Lewis Carroll

"If Quantum Computing ever really works Cryptography/SSL are in big trouble"

RSA Public Key Cryptography

RSA algorithm is based on the fact that
factorising large numbers* is ~~hard~~. *slow*

*semi-prime

Naïve Serial Factorization Algorithm using (modulo) division

```
def find_factor(n):
    for c in range(2, int(math.sqrt(n))):
        if n % c == 0:
            return c
    return None
```

RSA Public Key Cryptography

Naïve Serial Factorization Algorithm
using only multiplication

```
def check_factors(n, f1, f2):
    return f1 * f2 == n


def find_factors(n):
    for f1 in range(2, int(math.sqrt(n))):
        for f2 in range(int(math.sqrt(n)), n // 2):
            if check_factors(n, f1, f2):
                return (f1, f2)
    return None
```

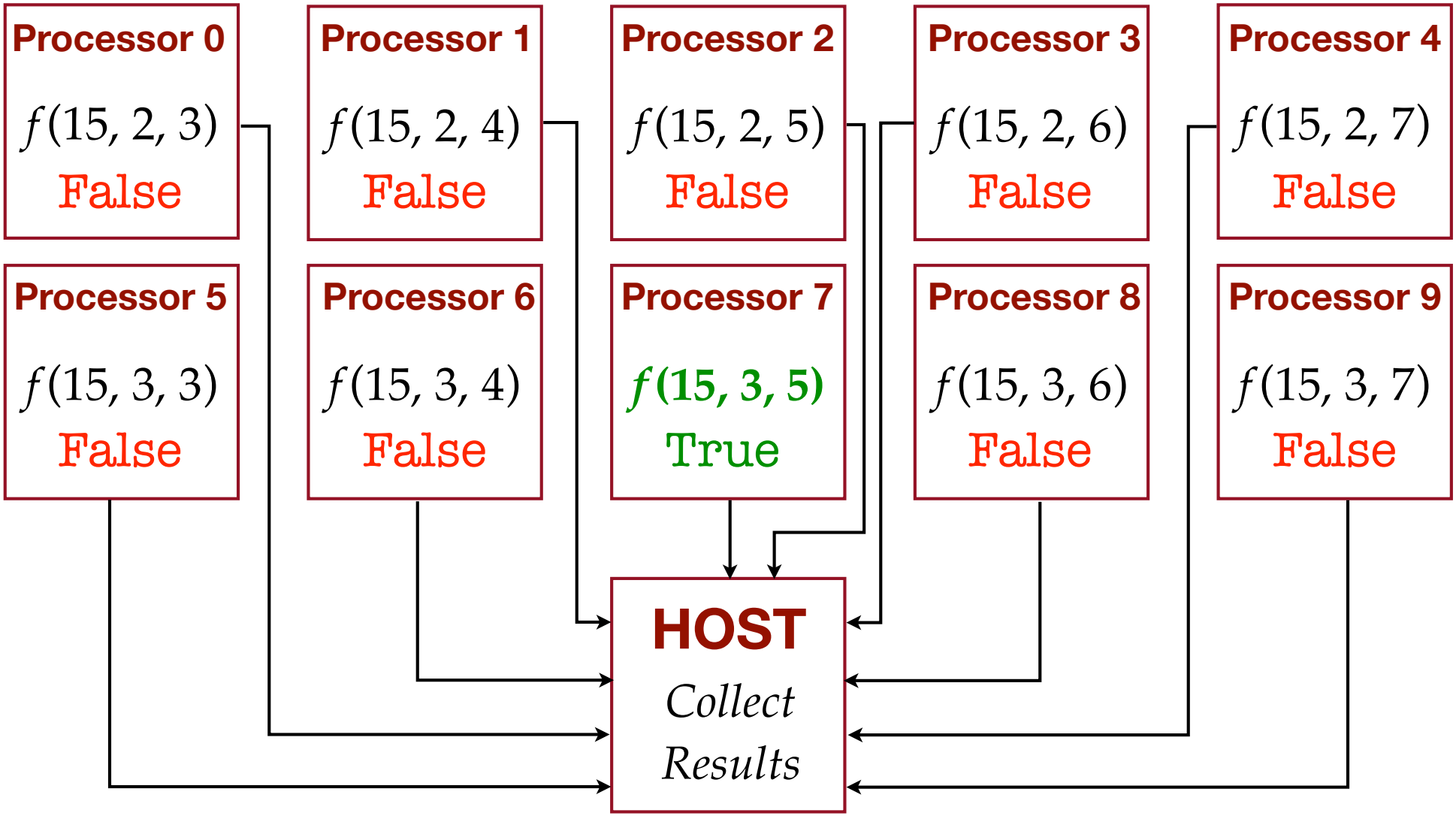
RSA Public Key Cryptography

Naïve Parallel Solution (*with* $f =$ `check_factors`)

Processor 0 $f(15, 2, 3)$ False	**Processor 1** $f(15, 2, 4)$ False	**Processor 2** $f(15, 2, 5)$ False	**Processor 3** $f(15, 2, 6)$ False	**Processor 4** $f(15, 2, 7)$ False
Processor 5 $f(15, 3, 3)$ False	**Processor 6** $f(15, 3, 4)$ False	**Processor 7** $f(15, 3, 5)$ True	**Processor 8** $f(15, 3, 6)$ False	**Processor 9** $f(15, 3, 7)$ False

RSA Public Key Cryptography

Naïve Parallel Solution (*with* $f =$ `check_factors`)



Bits

BIT = Binary Digit **0** *or* **1**

Can set the value (write) and read the value
(or *state*) of the bit

The *same* bit can have
different values
at *different* times

Qubits

Qubit = Quantum Bit $|\mathbf{0}\rangle$ *or* $|\mathbf{1}\rangle$

or a mixture e.g. “$50\%|\mathbf{0}\rangle$ *and* $50\%|\mathbf{1}\rangle$”

which we can write as $\frac{1}{\sqrt{2}}|\mathbf{0}\rangle + \frac{1}{\sqrt{2}}|\mathbf{1}\rangle$

Qubits

$$\frac{1}{\sqrt{2}}|\mathbf{0}\rangle + \frac{1}{\sqrt{2}}|\mathbf{1}\rangle$$

A *single* qubit can have
different values
at *the same* time

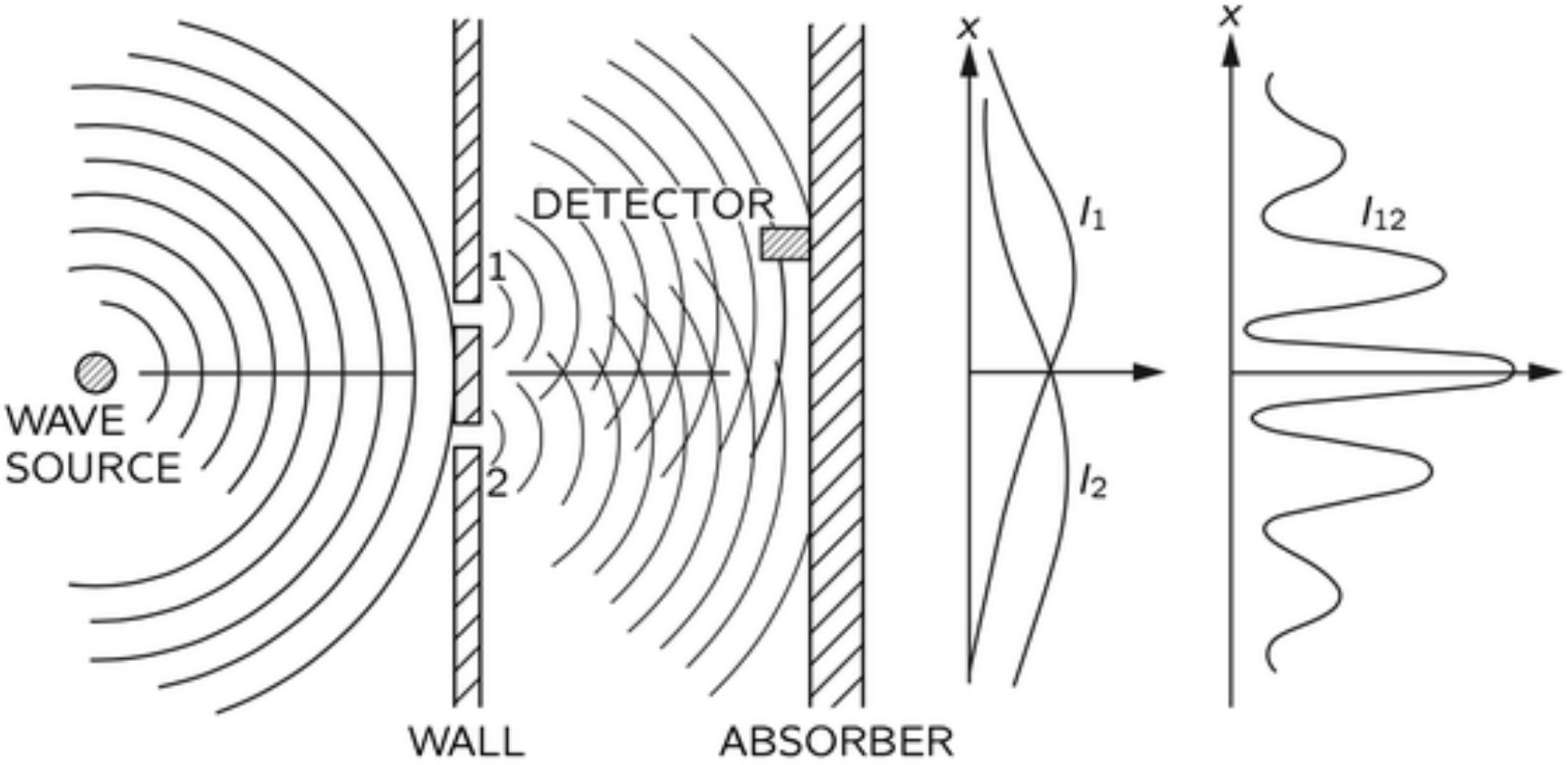
A SINGLE QUBIT
CAN HAVE
DIFFERENT VALUES
AT THE SAME TIME

starting-to-rain

. . . *that makes no sense*

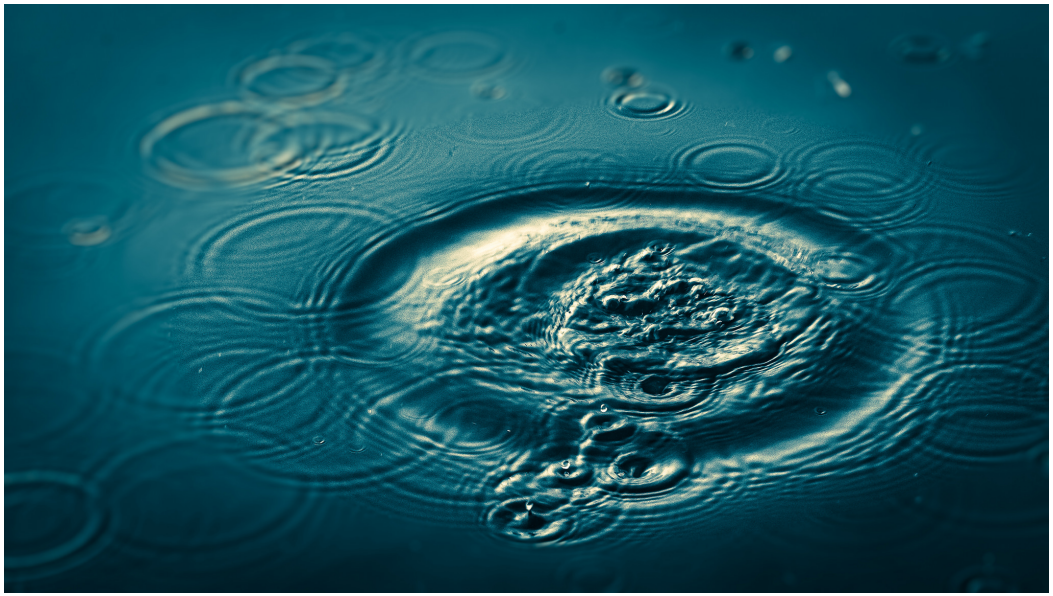
An experiment with waves

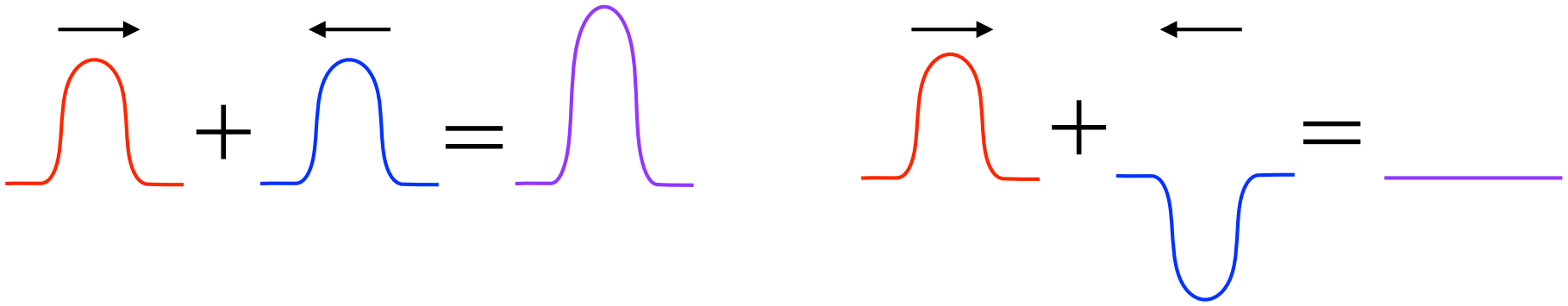
Thank you, Mr Feynman



The waves exhibit interference

Interference

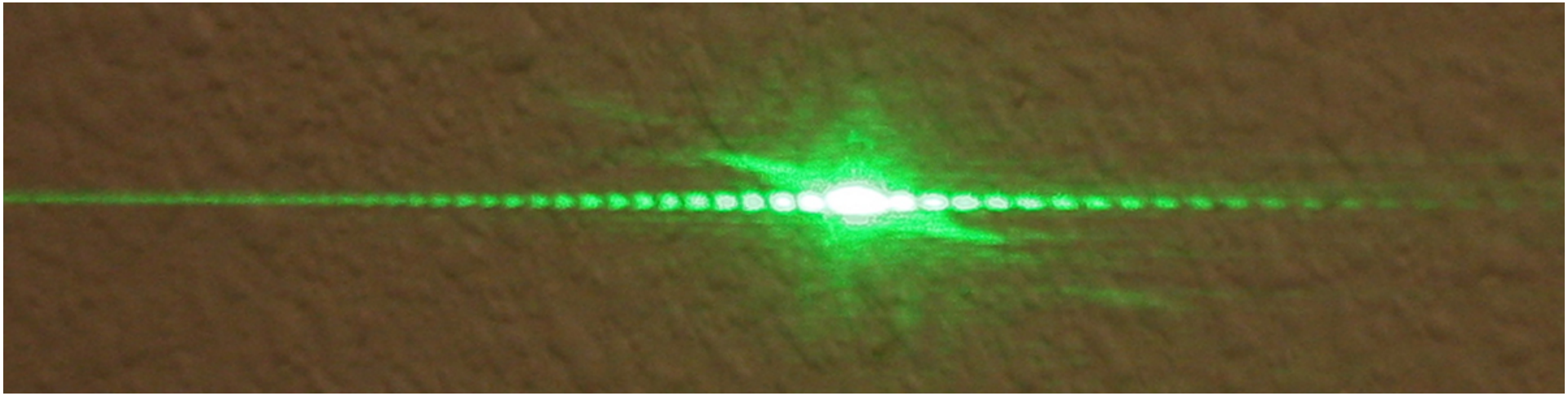




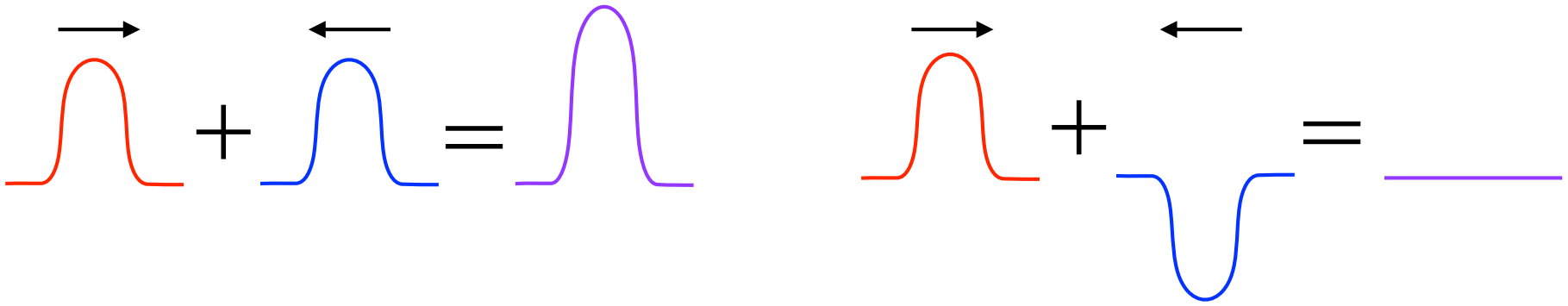
Constructive interference *Destructive interference*

(when the waves come together)

Interference



Science Experiment *(cropped & rotated)* *Copyright © Tom Brandt*

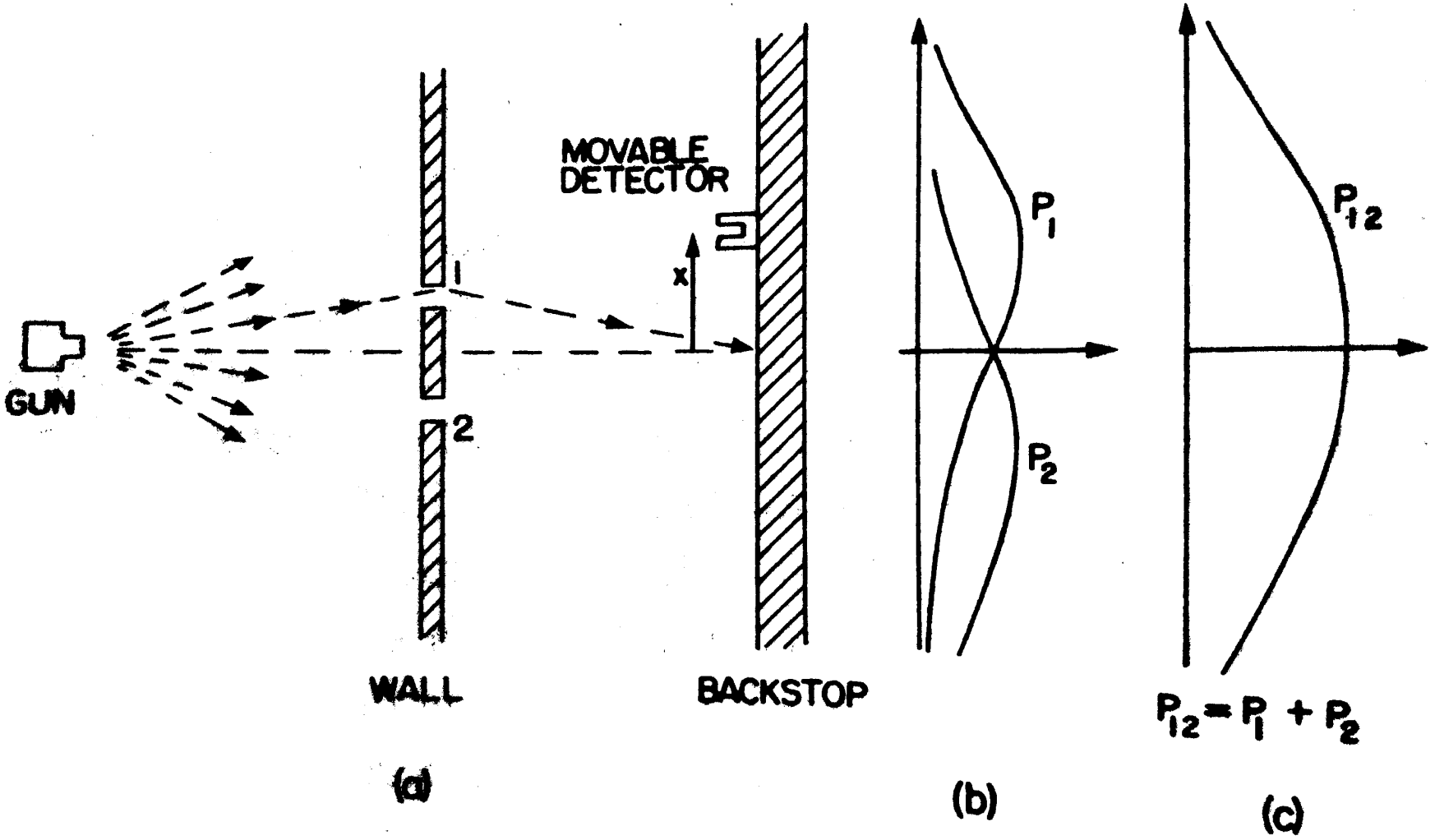


Constructive interference *Destructive interference*

(when the waves come together)

An experiment with bullets

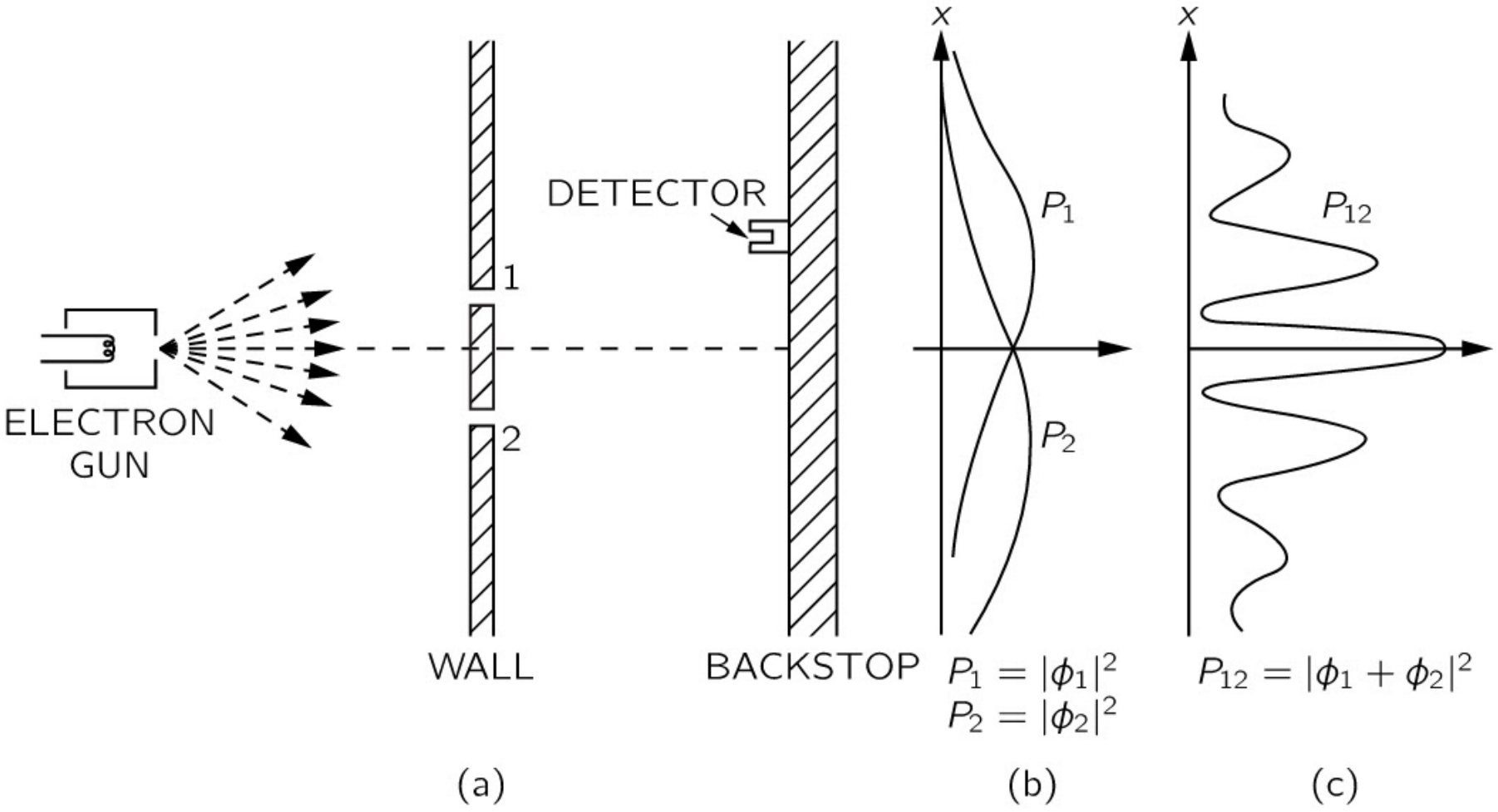
Thank you, Mr Feynman



*Bullets do **not** exhibit interference*

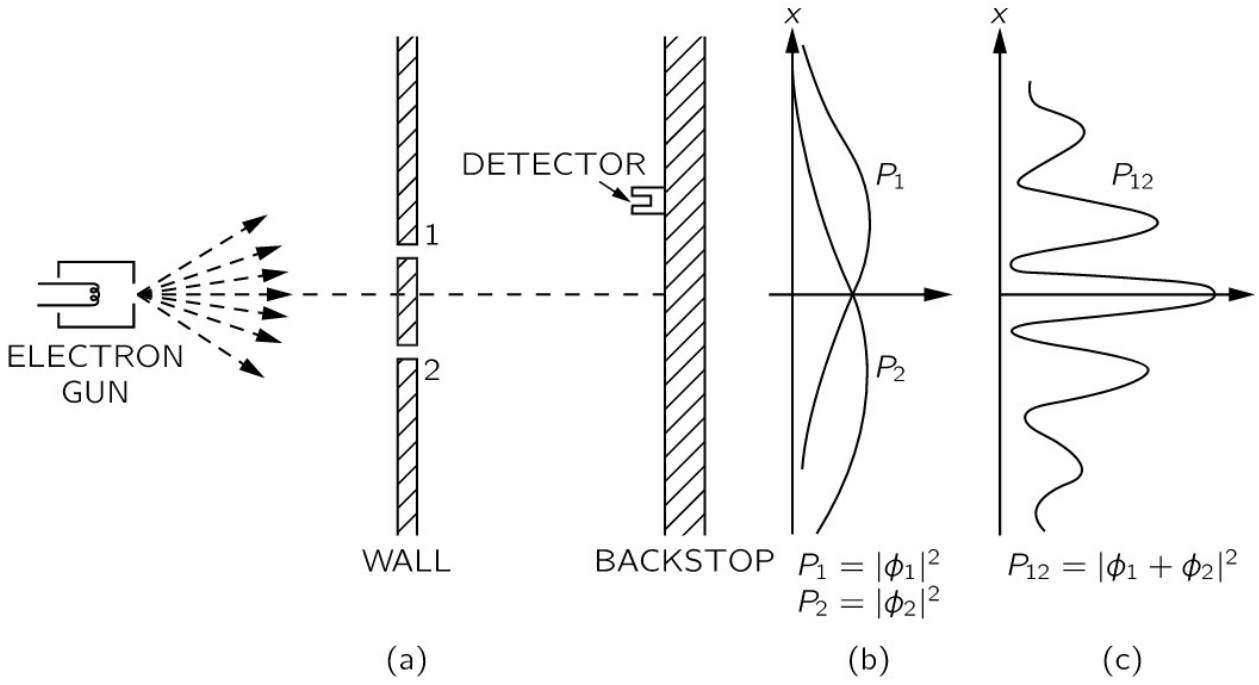
An experiment with electrons

Thank you, Mr Feynman



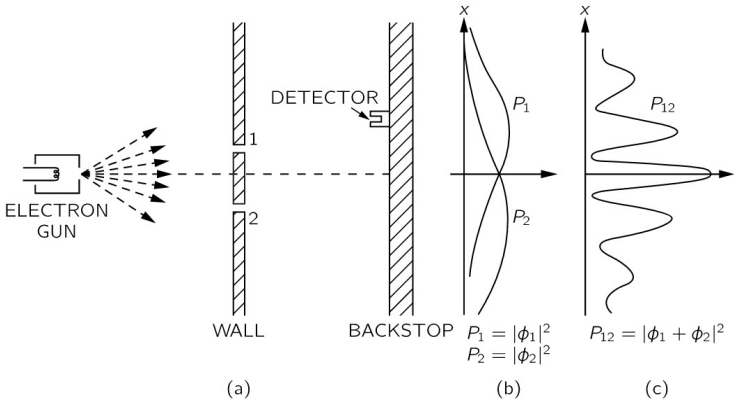
*Electrons **do** exhibit interference, **just like waves***

An experiment with electrons



If you reduce the electron gun power so that there is only ever one electron in the system at a time, the pattern ***remains***

An experiment with electrons



The electrons act ***as if*** *they were guided by waves that go through both slits and cause interference.*

Quantum mechanics describes particle motions with a wave equation for a (complex) wave, ψ, whose amplitude determines the probability of finding the particle at that position in spacetime.

Measurement

ψ can be in a mixed state (a superposition)

$$\psi = \frac{1}{\sqrt{2}} |\textbf{LEFT}\rangle + \frac{1}{\sqrt{2}} |\textbf{RIGHT}\rangle$$

Schrödinger's equation tells us how ψ evolves over time

Whenever we measure ψ, the wave function "collapses" and we get a definite answer

$$|\textbf{LEFT}\rangle \quad \textit{or} \quad |\textbf{RIGHT}\rangle$$

Measurement

$$\psi = \alpha|\mathbf{LEFT}\rangle + \beta|\mathbf{RIGHT}\rangle$$

When ψ is measured (ψ "collapses")

$$\text{Prob}\,(|\mathbf{LEFT}\rangle) = \alpha^*\alpha$$

$$\text{Prob}\,(|\mathbf{RIGHT}\rangle) = \beta^*\beta$$

ripple effects

that still

makes no sense

ripple effects

that still

makes no sense

*Quantum Mechanics**

* *Relativistic Quantum Field Theory*

Is the most accurate scientific theory ever.

There has never been a reproducible experiment
whose results contract the predictions
of quantum mechanics

Quantum mechanics has predicted phenomena
with an accuracy of ≈ 1 part in a billion

Interpretations

Many Worlds (Hugh Everett, 1957)

Whenever there are two or more quantum possibilities, the universe "branches" and all outcomes are realised in different universes

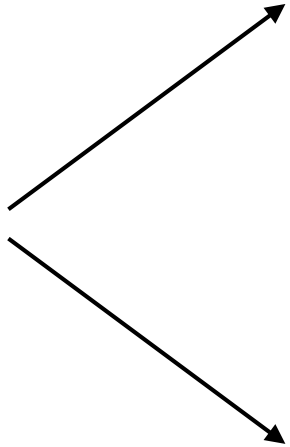
When we measure ψ, we get the value of ψ in our universe

But there is ***interference*** *between ψ in different universes!*

Interpretations

$$\psi = \alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle$$

Measure ψ:



In a proportion $\alpha^*\alpha$ of universes, we get $|\mathbf{0}\rangle$

In the other $\beta^*\beta$ $(= 1 - \alpha^*\alpha)$ proportion of universes, we get $|\mathbf{1}\rangle$

Bytes and Words

Byte = 8 bits

2^8 possible values

e.g. 0–255

Word = *n* bits (e.g. 64)

Entanglement

Multiple qubits can be "entangled"
(described by a single quantum state ψ)

$$\alpha_0|\mathbf{00000000}\rangle$$
$$+\alpha_1|\mathbf{00000001}\rangle$$
$$\vdots$$
$$+\alpha_n|\mathbf{11111111}\rangle$$

So is Quantum Computing a Parallel Computer Across Universes?

Universe 0 $f(15, 2, 3)$ False	**Universe 1** $f(15, 2, 4)$ False	**Universe 2** $f(15, 2, 5)$ False	**Universe 3** $f(15, 2, 6)$ False	**Universe 4** $f(15, 2, 7)$ False
Universe 5 $f(15, 3, 3)$ False	**Universe 6** $f(15, 3, 4)$ False	**Universe 7** $f(15, 3, 5)$ True	**Universe 8** $f(15, 3, 6)$ False	**Universe 9** $f(15, 3, 7)$ False

Kinda.

But there's a but.

BUT

*To benefit from Quantum Computing we need to find algorithms in which (nearly) all the answers we don't want cancel out (destructive interference), leaving the answer we do want in **all** universes (at least with reasonably high probability).*

That's what Shor's Algorithm does for large semi-prime numbers.

And it has been used on real quantum computers to factorize large-ish semi-primes.*

* *largest so far:* $21 = 3 \times 7$

Alternative Adiabatic Quantum Computer:
143 (= 11 × 13)

It was later discovered it had also
factorized (56,153 = 233 × 241)

```
$ time python factorize.py 56153
real 0m0.052s
user 0m0.037s
sys  0m0.012s

$ time python factorize2.py 56153
real 0m1.165s
user 0m1.147s
sys  0m0.015s
```

* *single core!*

Summary

The physics is 100% sound: Quantum Computing is based on our absolute best physics

The engineering is . . . tricky

Quantum Computers currently "decohere" quickly, because of other stuff in the universe(s), and we can't yet have many qubits

They're probably coming . . . but they'll be tricky to program

Shor's Algorithm

Don't attack factorisation directly.

This sequence is periodic (repeats) for almost any x:

$x \pmod N,\ x^2 \pmod N,\ x^3 \pmod N,\ \ldots,\ x^k \pmod N,\ \ldots$

$N = p_1 p_2$
(the number to factorize)

[$x \pmod N$ = `x % N`]

If we can find the period of such sequences for a few values of x, we can find p_1 & p_2

— *Euler*

Shor's Algorithm

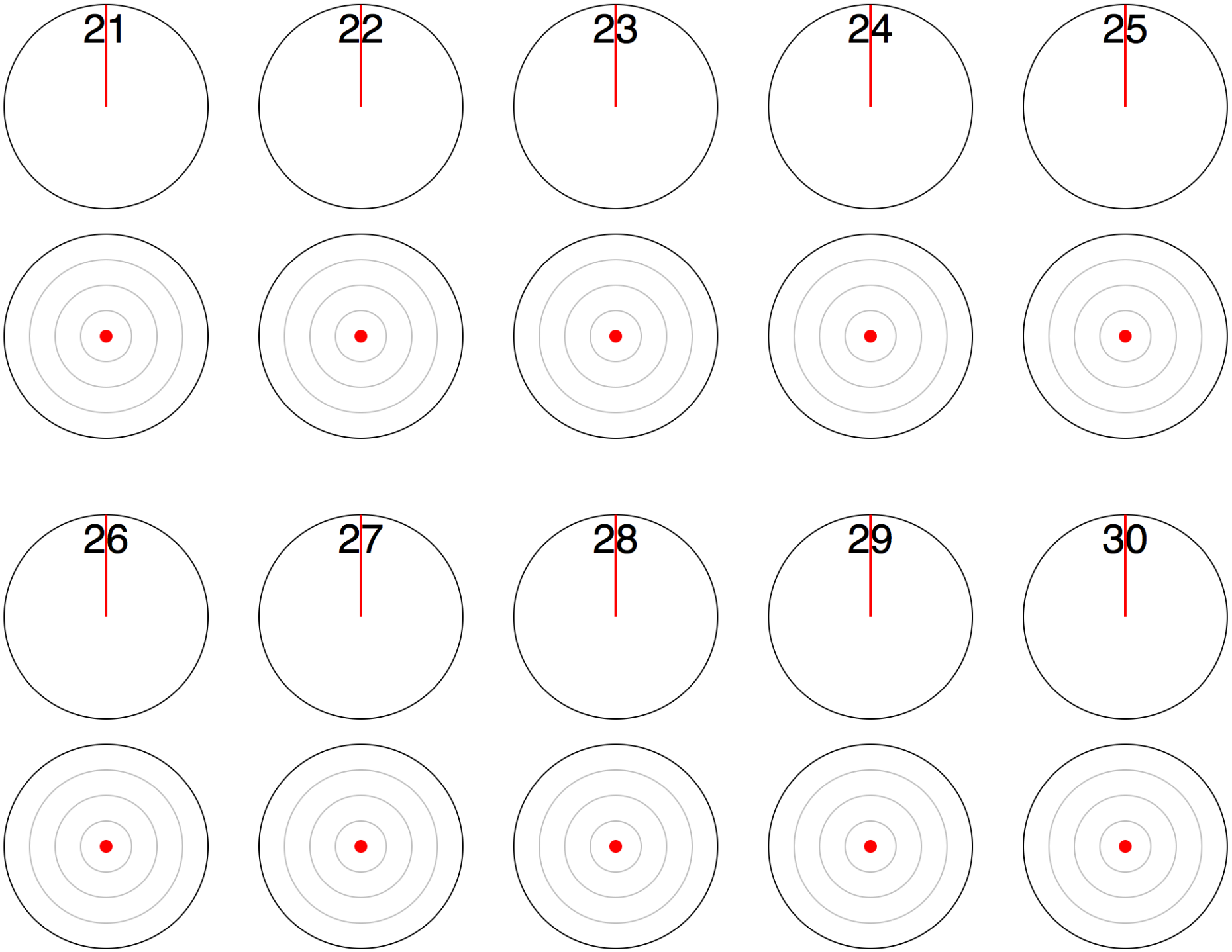
We form a quantum superposition of the elements of the sequence

$x \pmod N$, $x^2 \pmod N$, $x^3 \pmod N$, … , $x^k \pmod N$, …

Use Quantum Fourier Transform to find the period, as a global property of the sequence.

Because it's global, we can read the period in ***any*** *universe — in particular,* ***ours****!*

Will attempt to illustrate using an idea by Scott Aaronson


21
22
23
24
25
26
27
28
29
30

@njr0

njr@StochasticSolutions.com

Universe: `4c4b59c9-e2a1-42ae-87f5-56290aadd071`

Credits and References

Mathematical Disturbance	*Andrew Newill*		*https://www.flickr.com/photos/andrewnewill/35855735601*
starting-to-rain	*Neil Tackaberry*		*https://www.flickr.com/photos/23629083@N03/16634435111*
Science Experiment	*Tom Brandt*		*https://www.flickr.com/photos/12567713@N00/17960280549*
An Experiment with Waves	*Richard Feynman, Robert Leighton, & Matthew Sands*	*Copyright (fair use)*	*The Feynman Lectures on Physics, Vol III: Quantum Mechanics*
An Experiment with Bullets			
An Experiment with Electrons			
ripple effects	*PsJeremy*		*https://www.flickr.com/photos/psjeremy/7451181596*
Quantum Clocks	*N J Radcliffe*		

Recommended Reading

Quantum Computing, A Gentle Introduction, Eleanor Rieffel & Wolfgang Polak, MIT Press (Cambridge, MA), 2014

The Feynman Lectures on Physics, Vol III: Quantum Mechanics, Richard P. Feynman, Robert B. Leighton & Matthew Sands, Addison-Wesley (Reading, MA), 1982

The Fabric of Reality, David Deutsch, Penguin (Harmondsworth), 1997 (esp. Chapter 9, Quantum Computers)