15-251: Great Theoretical Ideas in Computer Science
Lecture 25

Quantum Computation

Image: Centre for Quantum Photonics

WARNING

I DO NOT KNOW ANYTHING ABOUT PHYSICS.
SERIOUSLY.

Let me tell you about a certain scientific theory.

It hasn't been around that long
– since about the late '60s.

Too new for your parents to have learned it
when they were at school.

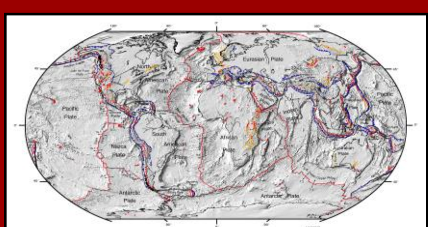
It's a bit hard to do direct experiments
to get evidence confirming the theory.

In the AskReddit thread *"What scientific 'fact' do you think may eventually be proven false?"* it was the #1 answer (1104 points).

The commenter (a scientist in the field), wrote:
"A lot of the theories behind [its] mechanisms… seem a little tenuous to me."

I'm talking, of course, about…

Plate Tectonics



Quantum Mechanics

on the other hand…

- has been standard physics for about 90 years
- has been confirmed by zillions of experiments
- is **relied upon** in the engineering of **hard drives**, **GPS devices**, **MRIs**, etc.

Please do not be skeptical of QM.

First 1/2 of lecture:
Non-quantum stuff

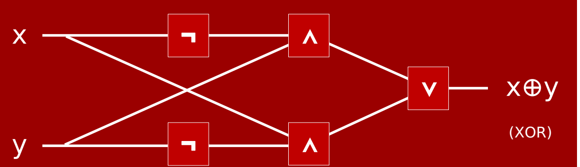
Late ’30s: Boolean circuits


Nakashima

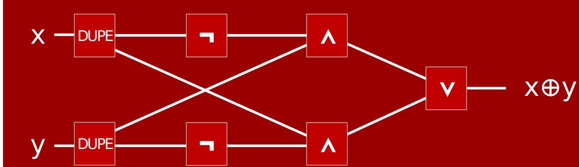

Shannon


Shestakov

Late ’30s: Boolean circuits



Late ’30s: Boolean circuits

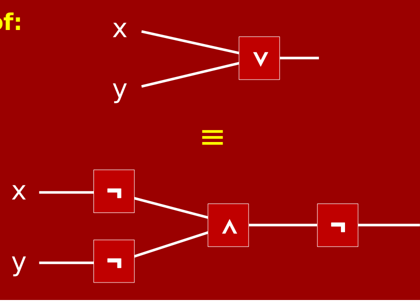


Fact: Every function $f : \{0,1\}^n \rightarrow \{0,1\}^m$ is computable with DUPE ¬ ∧ ∨

Fact: Every function $f : \{0,1\}^n \rightarrow \{0,1\}^m$ computable by a time-T algorithm can be computed by a circuit with poly(T) gates

Fact: Every function $f : \{0,1\}^n \rightarrow \{0,1\}^m$ is computable with DUPE ¬ ∧ ∨

Proof:



Fact: Every function f : $\{0,1\}^n \to \{0,1\}^m$ is computable with DUPE NAND and "scratch input bits"

Proof: Suffices to get ¬

x — ¬ —

≡

weirdo quantum notation

scratch bit, hardwired to 1 → ⟨1|

x, ⟨1| — NAND —

(alternative)

x — DUPE — NAND —

'60s: Reversible computation

Landauer

Bennett

(Remember Homework #1, Problem #4?)

Bit

In theory:	⟨0|	⟨1|
In practice:	low voltage	high voltage
	horizontally polarized photon	vertically polarized photon

Gate

A physical, localized gadget that manipulates a few bits.

? , ? — ∧ — ⟨0|

NOT reversible

Apparently, this means an AND gate **must** dissipate energy.

(Because physics. 2nd Law of Thermodynamics?)

Apparently, if a gate is **reversible**, it need not (in principle) dissipate energy.

— ¬ — **Reversible**

— ⊕ — **Not Reversible**

CNOT (controlled NOT): x — x, y — x⊕y **Reversible**

— DUPE — **Not Reversible** (we require #in = #out)

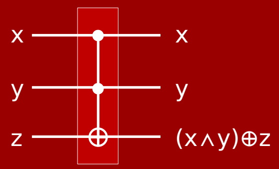
Question: Is every function f : $\{0,1\}^n \to \{0,1\}^m$ computable with only reversible gates?

Answer: **Yes!** (As you know from homework.)

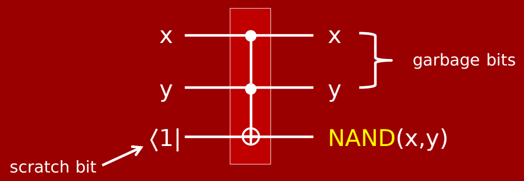
Need to allow some s scratch inputs, and g "garbage outputs".

Such that $n+s = m+g$.

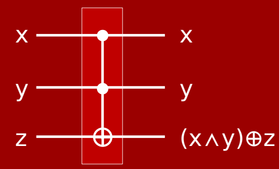
CCNOT
(aka *Toffoli* gate)



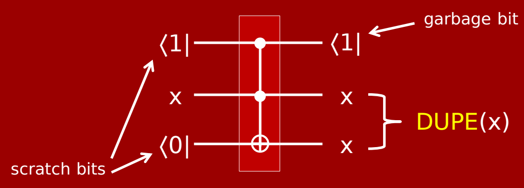
Reversible



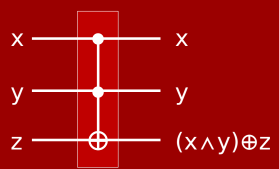
CCNOT
(aka *Toffoli* gate)



Reversible

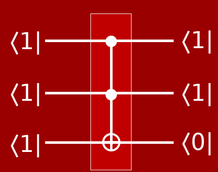


CCNOT
(aka *Toffoli* gate)

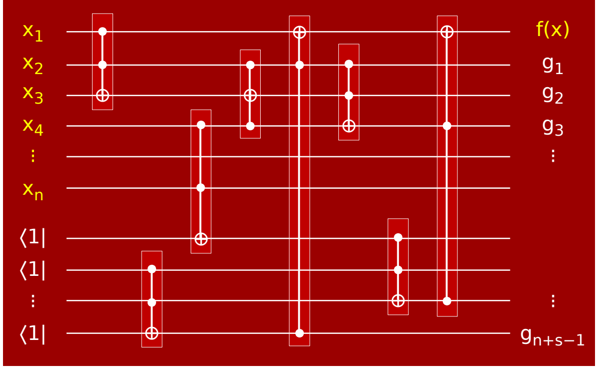


Reversible

If you prefer all scratch bits to be ⟨1|…



Any circuit for $f : \{0,1\}^n \to \{0,1\}$ can efficiently be converted into a reversible circuit.



Puzzle

Consider Multiply : $\{0,1\}^{n+n} \to \{0,1\}^{2n}$.
Takes two n-bit numbers and outputs product.
Can be done in poly(n) time.
Hence has a poly(n)-gate circuit.
Hence has a poly(n)-gate **reversible** circuit.

Why can't we just reverse the circuit, and get a poly(n)-gate circuit for **Factoring**?!

Solution: Have to know what garbage bits to feed in so that all scratch bits become ⟨1|.

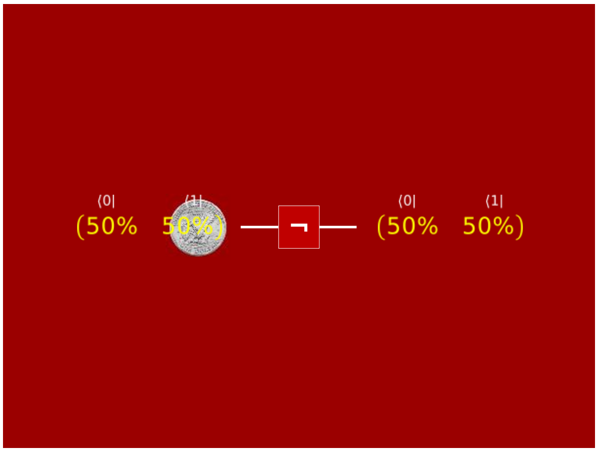
Late '70s: Probabilistic computation

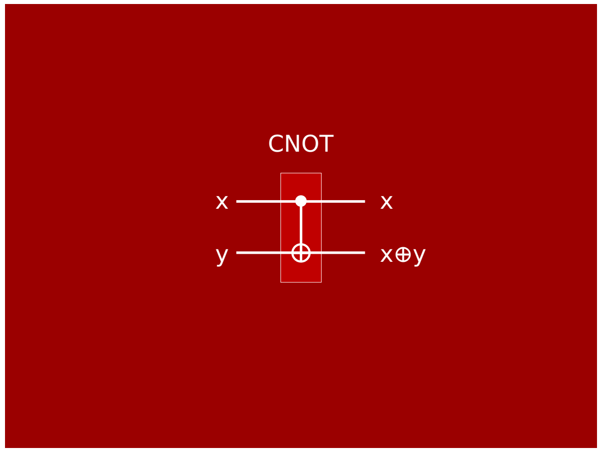

Rabin

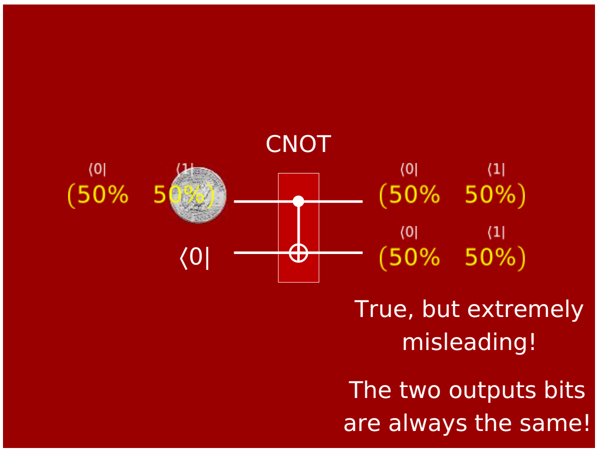

Solovay

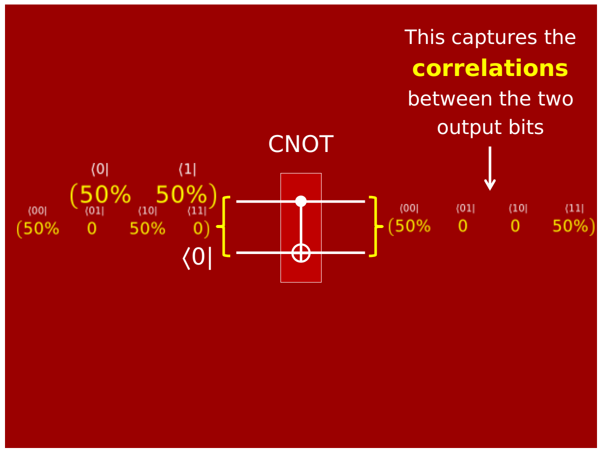

Strassen

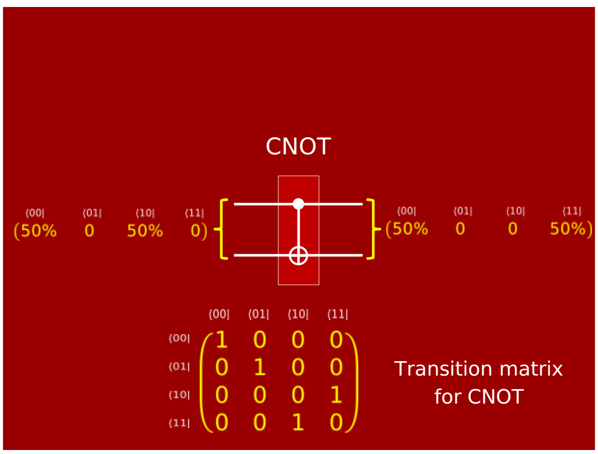

Gill

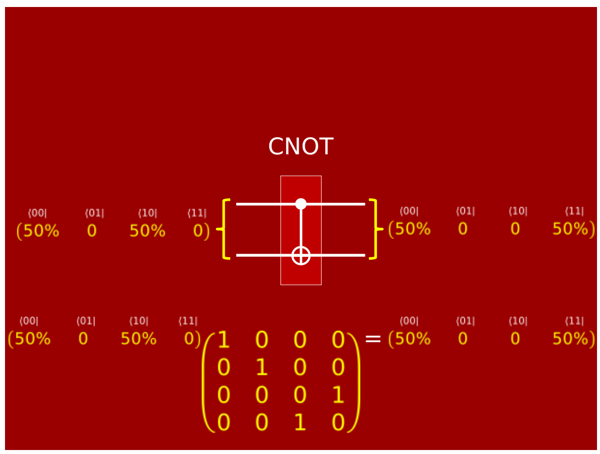

⟨0| ⟨1|
(50% 50%)
¬
⟨0| ⟨1|
(50% 50%)


CNOT
x
y
x
x⊕y

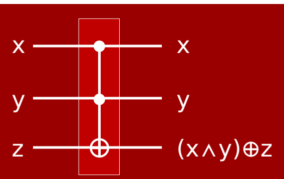

CNOT
⟨0| ⟨1|
(50% 50%)
⟨0|
⟨0| ⟨1|
(50% 50%)
⟨0| ⟨1|
(50% 50%)
True, but extremely misleading!
The two outputs bits are always the same!


This captures the
correlations
between the two output bits
CNOT
⟨0| ⟨1|
(50% 50%)
⟨00| ⟨01| ⟨10| ⟨11|
(50% 0 50% 0)
⟨0|
⟨00| ⟨01| ⟨10| ⟨11|
(50% 0 0 50%)


CNOT
⟨00| ⟨01| ⟨10| ⟨11|
(50% 0 50% 0)
⟨00| ⟨01| ⟨10| ⟨11|
(50% 0 0 50%)
⟨00| ⟨01| ⟨10| ⟨11|
⟨00| 1 0 0 0
⟨01| 0 1 0 0
⟨10| 0 0 0 1
⟨11| 0 0 1 0
Transition matrix for CNOT


CNOT
⟨00| ⟨01| ⟨10| ⟨11|
(50% 0 50% 0)
⟨00| ⟨01| ⟨10| ⟨11|
(50% 0 0 50%)
⟨00| ⟨01| ⟨10| ⟨11|
(50% 0 50% 0)
1 0 0 0
0 1 0 0
0 0 0 1
0 0 1 0
=
⟨00| ⟨01| ⟨10| ⟨11|
(50% 0 0 50%)

CCNOT (aka *Toffoli* gate)



$$
\begin{array}{c|cccccccc}
 & \langle 000| & \langle 001| & \langle 010| & \langle 011| & \langle 100| & \langle 101| & \langle 110| & \langle 111| \\
\hline
\langle 000| & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\langle 001| & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\langle 010| & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
\langle 011| & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
\langle 100| & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
\langle 101| & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
\langle 110| & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
\langle 111| & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{array}
$$

Transition matrix for CCNOT

A probabilistic gate I just made up

if ⟨0| do `Bern(.8)`
if ⟨1| do `Bern(.1)`

Sorta like ¬, but noisy (and asymmetric).

$$
\begin{array}{c|cc}
 & \langle 0| & \langle 1| \\
\hline
\langle 0| & .2 & .8 \\
\langle 1| & .9 & .1
\end{array}
$$

Transition matrix

In general:

A k-input/output probabilistic gate can be any $2^k \times 2^k$ **stochastic matrix** (matrix preserving prob. vectors).
I.e., each row nonnegative, sums to 1.

e.g.,

$$
\begin{array}{c|cccc}
 & \langle 00| & \langle 01| & \langle 10| & \langle 11| \\
\hline
\langle 00| & 0 & .2 & .7 & .1 \\
\langle 01| & 0 & .6 & .4 & 0 \\
\langle 10| & 0 & .1 & 0 & .9 \\
\langle 11| & 1 & 0 & 0 & 0
\end{array}
$$

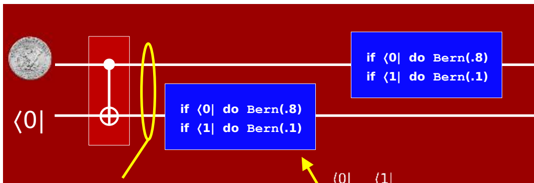
Here's one of the trickiest parts of the lecture.

It still has nothing to do with quantum.

What is the distribution of the 2 output wires?

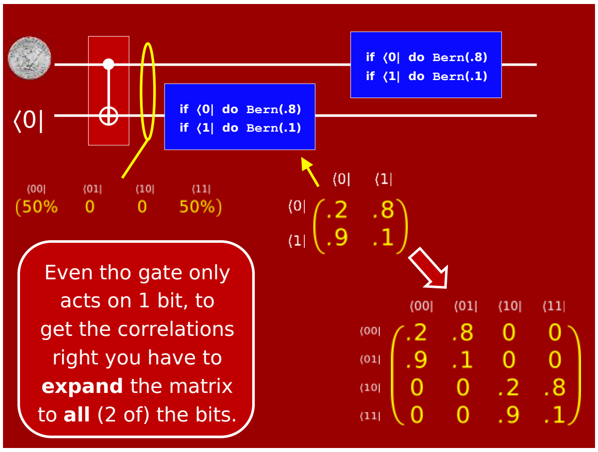
$$
\begin{array}{cccc}
\langle 00| & \langle 01| & \langle 10| & \langle 11| \\
(50\% & 0 & 50\% & 0)
\end{array}
\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}
=
\begin{array}{cccc}
\langle 00| & \langle 01| & \langle 10| & \langle 11| \\
(50\% & 0 & 0 & 50\%)
\end{array}
$$

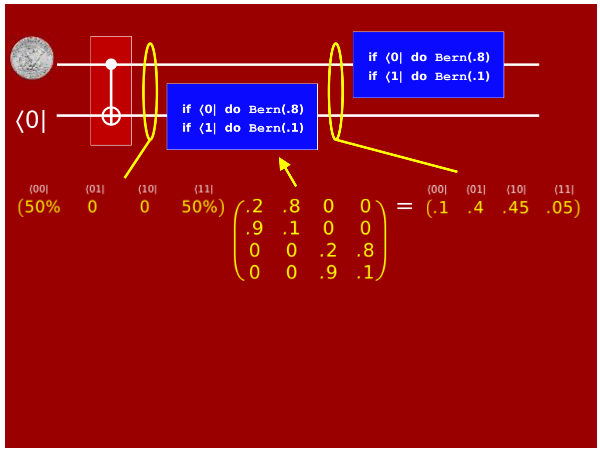
So far, we did this already.
(A few slides ago.)

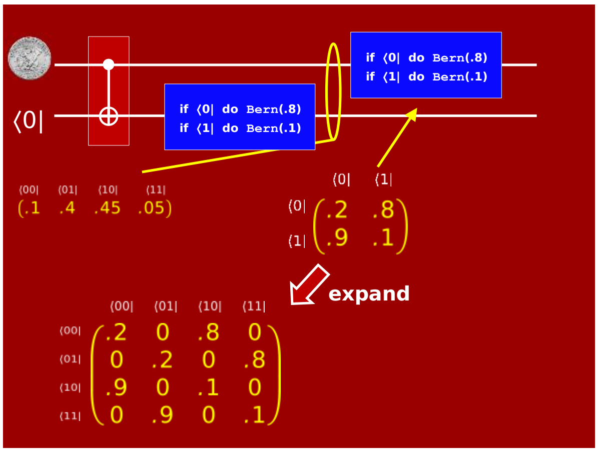


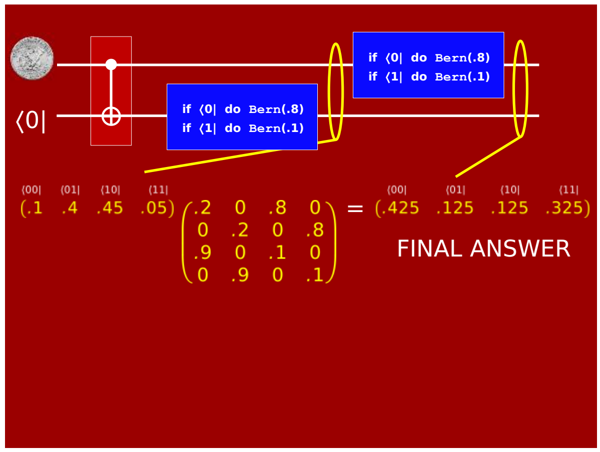
$$
\begin{array}{cccc}
\langle 00| & \langle 01| & \langle 10| & \langle 11| \\
(50\% & 0 & 0 & 50\%)
\end{array}
\qquad
\begin{array}{c|cc}
 & \langle 0| & \langle 1| \\
\hline
\langle 0| & .2 & .8 \\
\langle 1| & .9 & .1
\end{array}
$$

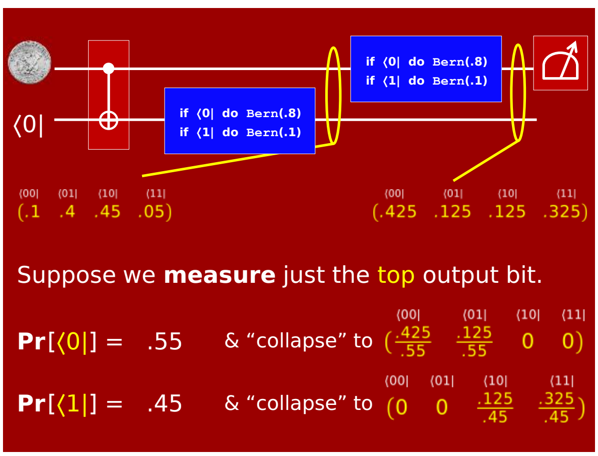
Type mismatch?

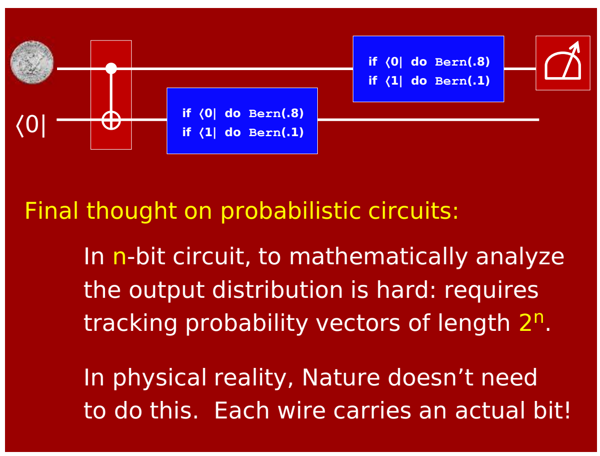

⟨0|
if ⟨0| do Bern(.8)
if ⟨1| do Bern(.1)
⟨00| ⟨01| ⟨10| ⟨11|
(50% 0 0 50%)
⟨0| ⟨1|
.2 .8
.9 .1
Even tho gate only acts on 1 bit, to get the correlations right you have to expand the matrix to all (2 of) the bits.
.2 .8 0 0
.9 .1 0 0
0 0 .2 .8
0 0 .9 .1


⟨0|
if ⟨0| do Bern(.8)
if ⟨1| do Bern(.1)
(50% 0 0 50%)
.2 .8 0 0
.9 .1 0 0
0 0 .2 .8
0 0 .9 .1
=
(.1 .4 .45 .05)


⟨0|
if ⟨0| do Bern(.8)
if ⟨1| do Bern(.1)
(.1 .4 .45 .05)
.2 .8
.9 .1
expand
.2 0 .8 0
0 .2 0 .8
.9 0 .1 0
0 .9 0 .1


⟨0|
if ⟨0| do Bern(.8)
if ⟨1| do Bern(.1)
(.1 .4 .45 .05)
.2 0 .8 0
0 .2 0 .8
.9 0 .1 0
0 .9 0 .1
=
(.425 .125 .125 .325)
FINAL ANSWER


⟨0|
if ⟨0| do Bern(.8)
if ⟨1| do Bern(.1)
(.1 .4 .45 .05)
(.425 .125 .125 .325)
Suppose we measure just the top output bit.
Pr[⟨0|] = .55 & "collapse" to (.425/.55 .125/.55 0 0)
Pr[⟨1|] = .45 & "collapse" to (0 0 .125/.45 .325/.45)


⟨0|
if ⟨0| do Bern(.8)
if ⟨1| do Bern(.1)
Final thought on probabilistic circuits:
In n-bit circuit, to mathematically analyze the output distribution is hard: requires tracking probability vectors of length 2^n.
In physical reality, Nature doesn't need to do this. Each wire carries an actual bit!

Finally: Quantum computation is exactly the same as this, except…

The state vectors can have **negative** entries!

Instead of being called "probabilities", the state vector entries are called "**amplitudes**".

Instead of the entries adding up to 1, the **squares** of the entries must add up to 1.

'80s and '90s: Quantum computation


Feynman


Deutsch

Bit

In theory: $\langle 0|$ $\langle 1|$

Physically: horizontally polarized photon; vertically polarized photon

According to the *actual* laws of physics (QM), a photon's state can be any **superposition**:

$$\alpha\,\langle 0| + \beta\,\langle 1|$$

where $\alpha, \beta \in \mathbb{R}$ satisfy $\alpha^2+\beta^2 = 1$.

Actually, according to quantum mechanics, the amplitudes can even be **complex numbers**.

I.e., we can have $\alpha,\beta \in \mathbb{C}$ satisfying $|\alpha|^2+|\beta|^2 = 1$.

However, for quantum computation purposes, it's known that real amplitudes suffice (WLOG).

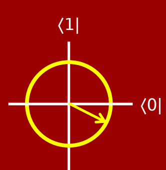
So let's keep things simple.

A qubit

$\alpha\,\langle 0| + \beta\,\langle 1|$ where "amplitudes" $\alpha, \beta \in \mathbb{R}$ satisfy $\alpha^2+\beta^2 = 1$.

Also written as a vector $\begin{array}{cc} \langle 0| & \langle 1| \\ \end{array}$ $\begin{pmatrix} \alpha & \beta \end{pmatrix}$

satisfying: $\left\| \begin{pmatrix} \alpha & \beta \end{pmatrix} \right\|^2 = 1$



It's NOT a probabilistic mixture of $\langle 0|$ and $\langle 1|$. It just is what it is.

2 qubits

$\begin{array}{cc} \langle 0| & \langle 1| \end{array}$ $\begin{pmatrix} \alpha & \beta \end{pmatrix}$

$\begin{array}{cc} \langle 0| & \langle 1| \end{array}$ $\begin{pmatrix} \alpha' & \beta' \end{pmatrix}$

Joint state if they're "prepared separately":

$\begin{array}{cccc} \langle 00| & \langle 01| & \langle 10| & \langle 11| \end{array}$ $\begin{pmatrix} \alpha\alpha' & \alpha\beta' & \beta\alpha' & \beta\beta' \end{pmatrix}$

Same rule as if they were independent probabilities.

Check: $(\alpha\alpha')^2 + (\alpha\beta')^2 + (\alpha'\beta)^2 + (\alpha'\beta')^2$
$= (\alpha^2+\beta^2)\cdot(\alpha'^2+\beta'^2)$
$= 1\cdot 1 = 1$

2 qubits

In general, 2 qubits can be in *any* superposition

$$\alpha \langle 00| + \beta \langle 01| + \gamma \langle 10| + \delta \langle 11|$$

where amplitudes satisfy $\alpha^2+\beta^2+\gamma^2+\delta^2 = 1$.

Also written as a vector: $\begin{array}{cccc} \langle 00| & \langle 01| & \langle 10| & \langle 11| \\ (\alpha & \beta & \gamma & \delta) \end{array}$

satisfying: $\left\| (\alpha \;\; \beta \;\; \gamma \;\; \delta) \right\|^2 = 1$

2 qubits

Example: $\frac{1}{\sqrt{2}}\langle 00| + \frac{1}{\sqrt{2}}\langle 11|$ ("EPR pair")

aka $\begin{array}{cccc} \langle 00| & \langle 01| & \langle 10| & \langle 11| \\ (\frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}}) \end{array}$

Fact: **Not** of form $\begin{array}{cccc} \langle 00| & \langle 01| & \langle 10| & \langle 11| \\ (\alpha\alpha' & \alpha\beta' & \alpha'\beta & \beta\beta') \end{array}$

Hence these two qubits are called **entangled**.

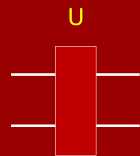
n qubits

State can be any 2^n-dimensional vector v satisfying $||v||^2 = 1$.

Coordinates indexed as $v_{\langle x|}$ for x ranging in $\{0,1\}^n$.

Quantum gates

$\begin{array}{cccc} \langle 00| & \langle 01| & \langle 10| & \langle 11| \\ (\alpha & \beta & \gamma & \delta) \end{array}$



$\begin{array}{cccc} \langle 00| & \langle 01| & \langle 10| & \langle 11| \\ (\alpha & \beta & \gamma & \delta) \end{array} \cdot U$

Gate is again represented by some 4×4 matrix.

$\begin{array}{c|cccc} & \langle 00| & \langle 01| & \langle 10| & \langle 11| \\ \langle 00| & & & & \\ \langle 01| & & & & \\ \langle 10| & & U & & \\ \langle 11| & & & & \end{array}$

Can be any U satisfying "$||vU||^2 = 1$ whenever $||v||^2 = 1$".

Unitary matrices

"Length-preserving" matrices U, meaning $||vU||^2 = 1$ whenever $||v||^2 = 1$, are called **unitary**.

Fact: An equivalent condition is:

$$UU^\dagger = I$$

"(conjugate) transpose" of U: switch ij and ji entries
(and take complex conjugates)

matrix with 1's on diagonal, 0's elsewhere

Unitary matrices

"Length-preserving" matrices U, meaning $||vU||^2 = 1$ whenever $||v||^2 = 1$, are called **unitary**.

Fact: An equivalent condition is:

$$UU^\dagger = I$$
$$\Leftrightarrow$$
$$U^{-1} = U^\dagger$$
$$\Rightarrow$$
U is reversible

Example quantum gates

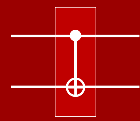
$$\begin{array}{cc} \langle 0| & \langle 1| \\ \hline \end{array}\!\!\!\!\!\!\!\!\begin{pmatrix} \alpha & \beta \end{pmatrix} \;—\boxed{\neg}—\; \begin{pmatrix} \beta & \alpha \end{pmatrix}$$

$$\begin{array}{c|cc} & \langle 0| & \langle 1| \\ \langle 0| & 0 & 1 \\ \langle 1| & 1 & 0 \end{array}$$

Example quantum gates

CNOT

$$\begin{array}{cccc} \langle 00| & \langle 01| & \langle 10| & \langle 11| \\ \alpha & \beta & \gamma & \delta \end{array}$$

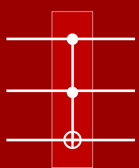


$$\begin{array}{cccc} \langle 00| & \langle 01| & \langle 10| & \langle 11| \\ \alpha & \beta & \delta & \gamma \end{array}$$

$$\begin{array}{c|cccc} & \langle 00| & \langle 01| & \langle 10| & \langle 11| \\ \langle 00| & 1 & 0 & 0 & 0 \\ \langle 01| & 0 & 1 & 0 & 0 \\ \langle 10| & 0 & 0 & 0 & 1 \\ \langle 11| & 0 & 0 & 1 & 0 \end{array}$$

Example quantum gates

CCNOT



$$\begin{array}{c|cccccccc} & \langle 000| & \langle 001| & \langle 010| & \langle 011| & \langle 100| & \langle 101| & \langle 110| & \langle 111| \\ \langle 000| & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \langle 001| & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \langle 010| & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \langle 011| & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ \langle 100| & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ \langle 101| & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ \langle 110| & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ \langle 111| & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}$$

Example quantum gates

The crucially important “Hadamard gate”:

$$\begin{array}{cc} \langle 0| & \langle 1| \\ \alpha & \beta \end{array} \;—\boxed{\mathbf{H}}—\; \begin{array}{cc} \langle 0| & \langle 1| \\ \frac{1}{\sqrt2}\alpha + \frac{1}{\sqrt2}\beta & \frac{1}{\sqrt2}\alpha - \frac{1}{\sqrt2}\beta \end{array}$$

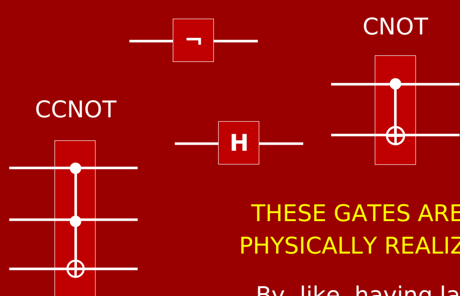
$$\mathbf{H} = \begin{array}{c|cc} & \langle 0| & \langle 1| \\ \langle 0| & \frac{1}{\sqrt2} & \frac{1}{\sqrt2} \\ \langle 1| & \frac{1}{\sqrt2} & -\frac{1}{\sqrt2} \end{array}$$

Example quantum gates

$$\langle 0| \;—\boxed{\mathbf{H}}—\; \frac{1}{\sqrt2}\langle 0| + \frac{1}{\sqrt2}\langle 1| \;—\boxed{\mathbf{H}}—\; \langle 0|$$

$$\mathbf{H} = \begin{array}{c|cc} & \langle 0| & \langle 1| \\ \langle 0| & \frac{1}{\sqrt2} & \frac{1}{\sqrt2} \\ \langle 1| & \frac{1}{\sqrt2} & -\frac{1}{\sqrt2} \end{array}$$

Example quantum gates



THESE GATES ARE ALL PHYSICALLY REALIZABLE

By, like, having lasers fired at the photons/qubits.

There are infinitely many
unitary matrices / possible gates.

But, just like DUPE+NAND for classical circuits…
and 50/50 coin flips for randomized circuits…

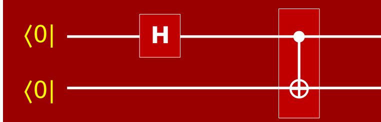

Yaoyun Shi
(施尧耘)

Theorem:

Without loss of generality,
quantum circuits only need
CCNOT and **Hadamard** gates.

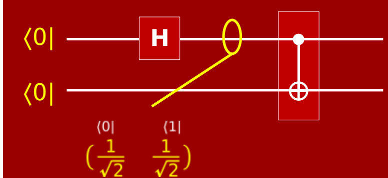
(It's convenient to also use **CNOT**.)

Example quantum circuit



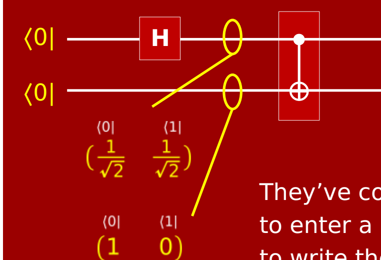
The qubits start out **separated**.
So it's okay to just apply **H** directly at first.

Example quantum circuit



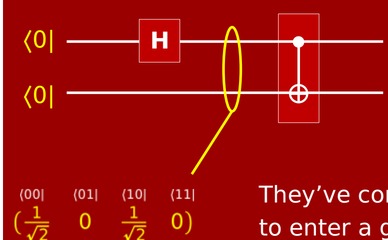
$$\mathbf{H} = \begin{array}{c c} & \begin{array}{cc} \langle 0| & \langle 1| \end{array} \\ \begin{array}{c} \langle 0| \\ \langle 1| \end{array} & \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \end{array}$$

Example quantum circuit



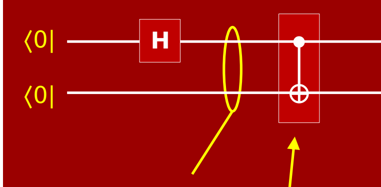
They've come together
to enter a gate. We need
to write them in joint state.

Example quantum circuit



They've come together
to enter a gate. We need
to write them in joint state.

Example quantum circuit

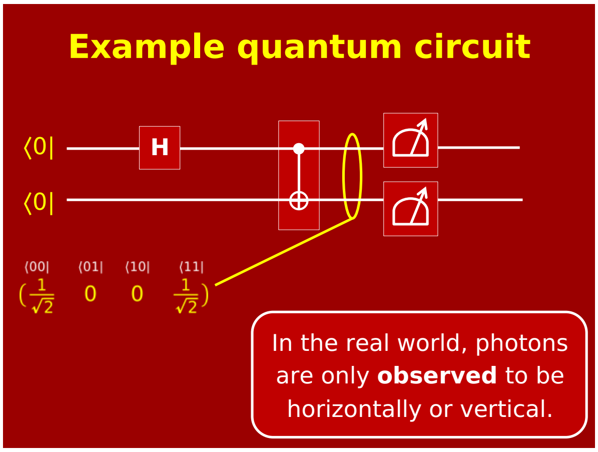


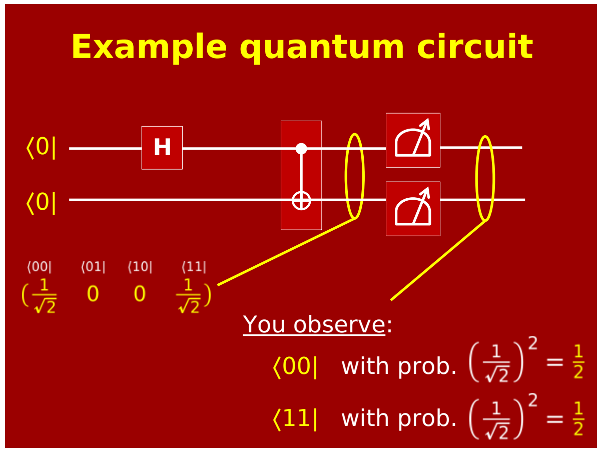
("EPR pair")

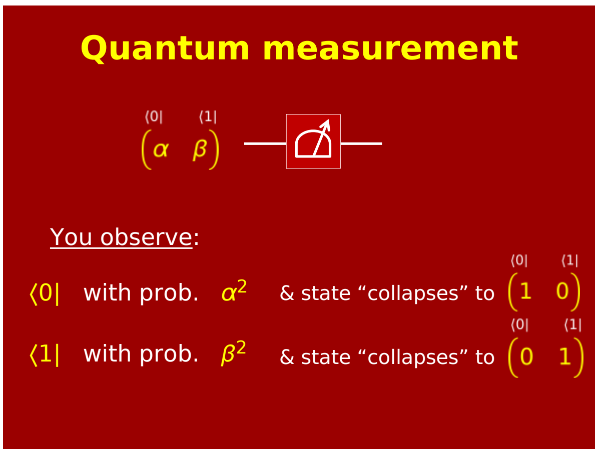
$\frac{1}{\sqrt{2}}\langle 00| + \frac{1}{\sqrt{2}}\langle 11|$

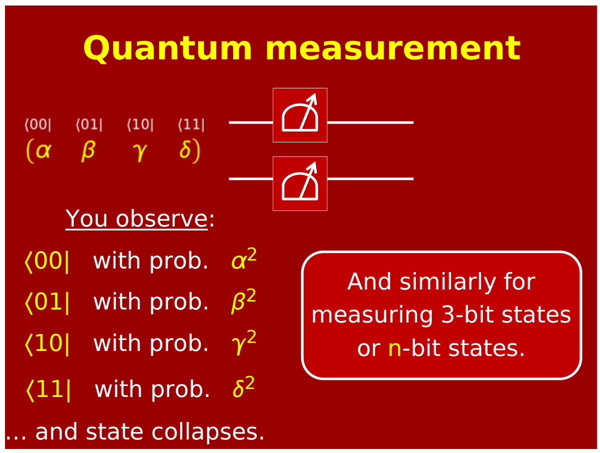
entangled

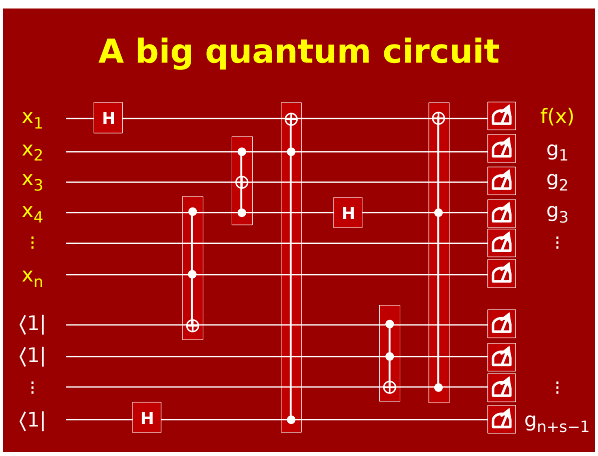
$$\begin{array}{cccc} \langle 00| & \langle 01| & \langle 10| & \langle 11| \end{array} \qquad\qquad \begin{array}{cccc} \langle 00| & \langle 01| & \langle 10| & \langle 11| \end{array}$$
$$\left(\tfrac{1}{\sqrt{2}} \quad 0 \quad \tfrac{1}{\sqrt{2}} \quad 0\right) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \left(\tfrac{1}{\sqrt{2}} \quad 0 \quad 0 \quad \tfrac{1}{\sqrt{2}}\right)$$

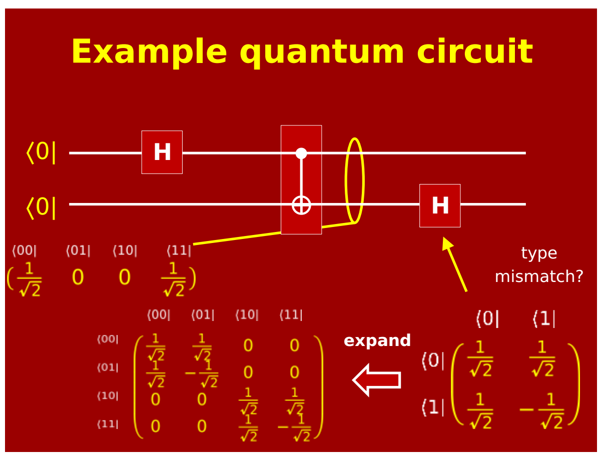

Example quantum circuit
⟨0|
⟨0|
H
⟨00| ⟨01| ⟨10| ⟨11|
$\left(\frac{1}{\sqrt{2}} \quad 0 \quad 0 \quad \frac{1}{\sqrt{2}}\right)$
In the real world, photons are only **observed** to be horizontally or vertical.


Example quantum circuit
⟨0|
⟨0|
H
⟨00| ⟨01| ⟨10| ⟨11|
$\left(\frac{1}{\sqrt{2}} \quad 0 \quad 0 \quad \frac{1}{\sqrt{2}}\right)$
You observe:
⟨00| with prob. $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$
⟨11| with prob. $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$

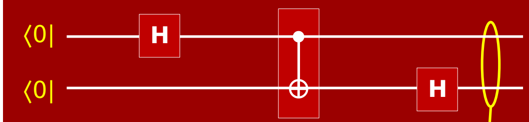

Quantum measurement
⟨0| ⟨1|
$(\alpha \quad \beta)$
You observe:
⟨0| with prob. α^2 & state "collapses" to ⟨0| ⟨1| $(1 \quad 0)$
⟨1| with prob. β^2 & state "collapses" to ⟨0| ⟨1| $(0 \quad 1)$


Quantum measurement
⟨00| ⟨01| ⟨10| ⟨11|
$(\alpha \quad \beta \quad \gamma \quad \delta)$
You observe:
⟨00| with prob. α^2
⟨01| with prob. β^2
⟨10| with prob. γ^2
⟨11| with prob. δ^2
… and state collapses.
And similarly for measuring 3-bit states or n-bit states.


A big quantum circuit
x_1
x_2
x_3
x_4
⋮
x_n
⟨1|
⟨1|
⋮
⟨1|
H
H
H
f(x)
g_1
g_2
g_3
⋮
⋮
g_{n+s-1}


Example quantum circuit
⟨0|
⟨0|
H
H
⟨00| ⟨01| ⟨10| ⟨11|
$\left(\frac{1}{\sqrt{2}} \quad 0 \quad 0 \quad \frac{1}{\sqrt{2}}\right)$
type mismatch?
expand
$$\begin{array}{c|cccc} & ⟨00| & ⟨01| & ⟨10| & ⟨11| \\ \hline ⟨00| & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ ⟨01| & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 \\ ⟨10| & 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ ⟨11| & 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{array}$$
$$\begin{array}{c|cc} & ⟨0| & ⟨1| \\ \hline ⟨0| & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ ⟨1| & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{array}$$

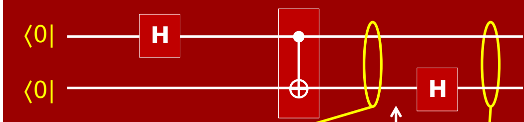
Example quantum circuit



$$\begin{array}{cccc} \langle 00| & \langle 01| & \langle 10| & \langle 11| \\ \end{array}$$
$$\left(\tfrac{1}{\sqrt{2}} \quad 0 \quad 0 \quad \tfrac{1}{\sqrt{2}}\right)\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

$$\begin{array}{ccccc} & \langle 00| & \langle 01| & \langle 10| & \langle 11| \\ = & \left(\tfrac{1}{2}\right. & \tfrac{1}{2} & \tfrac{1}{2} & \left.-\tfrac{1}{2}\right) \end{array}$$

Example quantum circuit

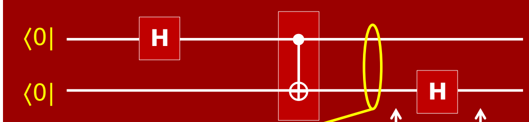


$$\begin{array}{cccc} \langle 00| & \langle 01| & \langle 10| & \langle 11| \\ \left(\tfrac{1}{\sqrt{2}}\right. & 0 & 0 & \left.\tfrac{1}{\sqrt{2}}\right) \end{array}$$

Alice takes first photon,
Bob takes second photon,
they fly light-years apart.

$$\begin{array}{cccc} \langle 00| & \langle 01| & \langle 10| & \langle 11| \\ \left(\tfrac{1}{2}\right. & \tfrac{1}{2} & \tfrac{1}{2} & \left.-\tfrac{1}{2}\right) \end{array}$$

Example quantum circuit



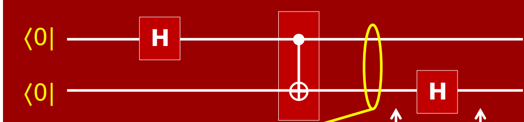
$$\begin{array}{cccc} \langle 00| & \langle 01| & \langle 10| & \langle 11| \\ \left(\tfrac{1}{\sqrt{2}}\right. & 0 & 0 & \left.\tfrac{1}{\sqrt{2}}\right) \end{array}$$

Bob applies gate, affects
Alice's qubit's state!

Alice takes first photon,
Bob takes second photon,
they fly light-years apart.

$$\begin{array}{cccc} \langle 00| & \langle 01| & \langle 10| & \langle 11| \\ \left(\tfrac{1}{2}\right. & \tfrac{1}{2} & \tfrac{1}{2} & \left.-\tfrac{1}{2}\right) \end{array}$$

Example quantum circuit



$$\begin{array}{cccc} \langle 00| & \langle 01| & \langle 10| & \langle 11| \\ \left(\tfrac{1}{\sqrt{2}}\right. & 0 & 0 & \left.\tfrac{1}{\sqrt{2}}\right) \end{array}$$

Bob applies gate, affects
Alice's qubit's state!

Alice takes first photon,
Bob takes second photon,
they fly light-years apart.

Spooky action at a distance.

Strange but true

In n-bit quantum circuit, to mathematically analyze the output state is hard: requires tracking state vectors of length 2^n.

In physical reality, Nature **does this**.

Unlike in probabilistic circuits, the qubits are not "secretly" in some definitive state.

They're really collectively in a giant superposition!

Experiments have confirmed this.

Why quantum computers?

1. Why not? Physics allows it.
2. [Feynman] Suppose the task you want to solve is "simulate a given quantum system."

   Seems to require exponential complexity with classical computers, trivial with quantum.
3. Other problems can be solved efficiently with quantum circuits, even though only known classical circuits have exponential complexity!

Shor's Algorithm

Peter Shor, 1994:

You can factor an n-bit number using $O(n^3)$-gate quantum circuit.

And thereby also crack RSA!

At this point, a **lot** of people became interested in building quantum computers!

Grover's Algorithm

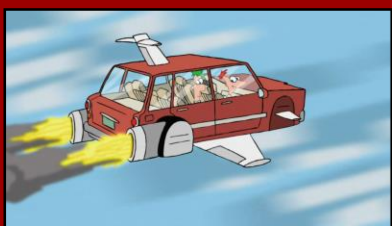
Lov Grover, 1996:

You can solve n-variable SAT using quantum circuit with $\approx 2^{n/2}$ gates.

Without quantum, believed to require $\approx 2^n$ gates.

The essence of Grover's algorithm is Homework #10 problem #5 ("Reflection Across The Average").

So… where are the quantum computers?!



And the flying cars, for that matter!?

So… where are the quantum computers?!

Well, they're working on it.

It's a hard engineering problem.

In 2012 they factored the number 21.

It's 3 × 7.

1840's

Babbage

Hey, I have an idea for an "Analytical Engine" (i.e., universal computing device).

It totally works great… in theory.

You're gonna need a lot of punch cards.

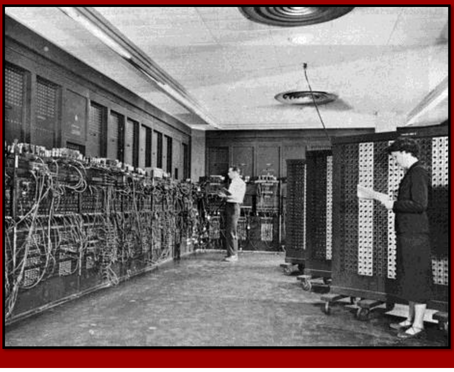
1840's

Lovelace

I wrote some code for that machine to compute the Bernoulli numbers.

This machine is going to be awesome once it gets built.

100 years later

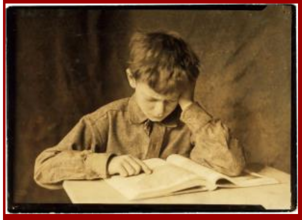


Moral of the story: Patience

In the meantime, Shor's algorithm is basically the only truly cool quantum algorithm we know.

So please, be a Lovelace.

Study Guide



Definitions:

CNOT and CCNOT gates.

Reversible computation.

Probabilistic circuits.

Quantum states.

Quantum measurement.

Skills:

Analyzing prob'istic circuits.

Expanding gate matrices.

Analyzing quantum circuits.