Lecture 26 – Time Travel

Let's reflect on what we've seen.

I started by telling you the laws of Q.M. seem to: a) be totally verified by experiment;
b) require nature to store exponentially much data.

Everett's Many Worlds Interpretation even suggests that 1500 particles leads to 10^{500} parallel universes.

His "academic sibling", David Deutsch took this 100% seriously and asked – "what can this do for computing?" In 1985 he posited general-purpose quantum computing, described a baby version of the Deutsch-Josza alg., and argued Q.C.'s would be able to get some exponential speedups over classical computers.

35 years later, mainstream major corporations & governments are spending 100's of millions of \$ building experimental Q.C.'s.... Theoretical Dreams → Practical Reality!

So... time travel. ☺

The "Einsten field equations" of G.R. are our best understanding of how space & time work.

In 1949, Kurt Gödel (of Incompleteness fame) showed $\exists$ solutions to the equations with "Closed Timelike Curves" (C.T.C.'s). I don't fully understand the meaning, but in short it would allow time-travelling particles. Maybe the simplest roughly-accurate explanation is:

You <u>could</u> have two points in spacetime

(t_0, x_0, y_0, z_0) $\quad$ (t_1, x_1, y_1, z_1)

such that –"by definition"– the state of particles at the two points is the same.

History sidebar: I recently learned Willem Jacob van Stockum discovered the same thing in 1937. A Dutch physicist who studied in Ireland, Canada (U. of T.!), and Scotland. Enlisted in Canadian Air Force in WWII, died in combat...

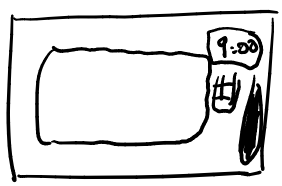
1973 Stephen Hawking & George F.R. Ellis:

"CTCs cannot logically exist b/c of the <u>Grandfather Paradox</u>".

→ a time-traveller goes back in time and kills their grandfather... (at a young age) so they never get born, so they never go back and kill their grandfather...

(A tiny bit like Cantor's Diagonalization argument!)

C.S. version:



time machine, shaped like a microwave oven

Can send one bit back in time, 9:01am → 9:00 am.

9:00am: you open microwave, get bit b_0

9:00-9:01: you apply NOT gate, producing b_1

9:01 am: you put b_1 in microwave

<u>Hawking & Ellis</u>: By def^{n} of CTC, $b_0 = b_1$

Case 1: $b_0 = 0$. Then $b_1 = NOT(0) = 1 \neq b_0$. ⇏⇐

Case 2: $b_0 = 1$. Then $b_1 = NOT(1) = 0 \neq b_0$. ⇏⇐.

CONTRADICTION!

Deutsch, 1991: "Not so fast....

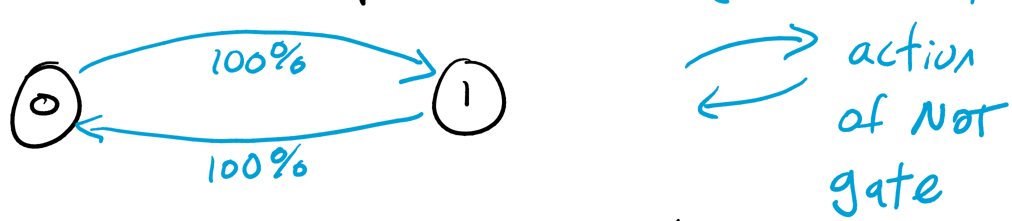
Laws of nature are Q.M. $\rightarrow$ randomness.

Suppose "state of b_0" is ⊛: "0 with prob. $\frac{1}{2}$,
1 with prob. $\frac{1}{2}$".

Then state of $b_1 = \text{NOT}(b_0)$ is "1 with prob. $\frac{1}{2}$,
0 with prob. $\frac{1}{2}$",

indeed the same as ⊛! No contradiction!

State Space:



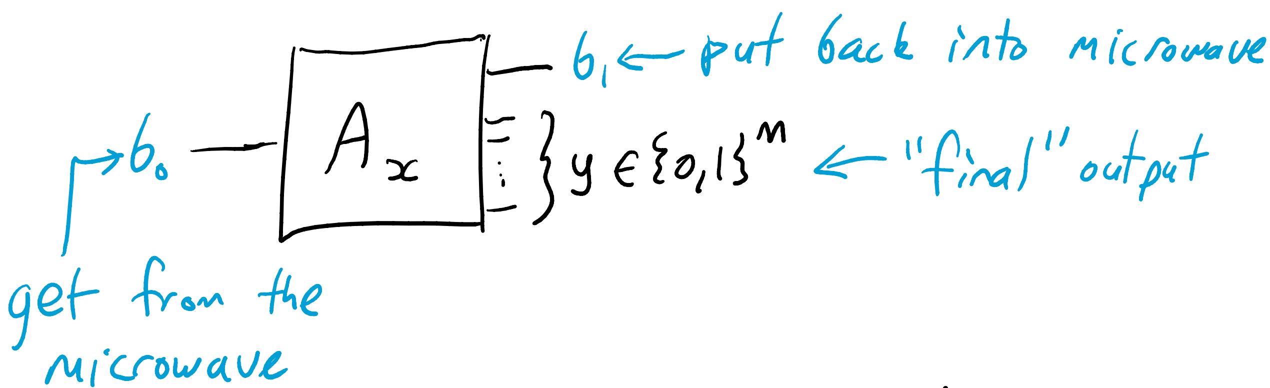
A (deterministic) "Markov chain", with
"steady state" = ⊛.
("invariant prob. distrib.")

Every Markov chain (or even the qubit analogue)
has a steady state $\Rightarrow$ never any
logical contradiction.

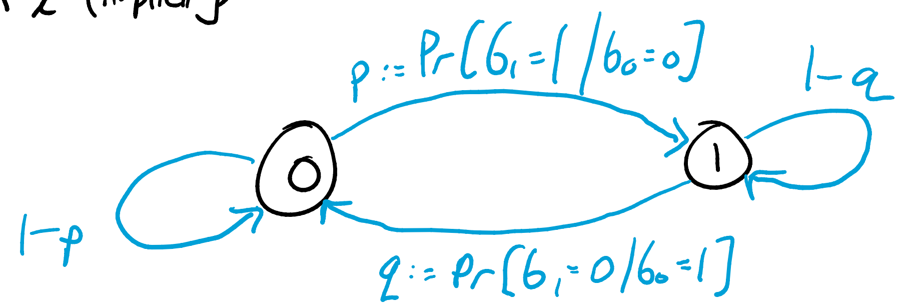
Deutsch, as always, asked: What computational power
could C.T.C.'s give us?

Deutschian model of computing with 1 time-travelling bit:

- Given input x, can make a circuit A_x (classical/randomized/quantum) with 1 input bits, $m+1$ output bits.

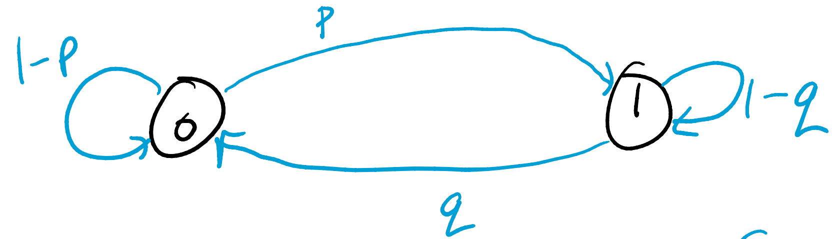


- A_x (implicitly) defines a 2-state Markov chain:



- Nature automagically sets distribution of b_0, b_1 to be (a) steady-state.
- A_x produces output y, assuming b_0 is input in this steady-state.

Remark: often just take $y := b_1$.



<u>Fact</u>: steady state is . . .
$$\sigma = \begin{cases} 0 & \text{w.prob. } \frac{q}{p+q} \\ 1 & \text{w. prob. } \frac{p}{p+q} \end{cases} \qquad (*)$$

<u>check</u>: Starting from $(*)$ and doing one step...

$$0 \text{ w. prob: } \frac{q}{p+q} \cdot \Pr[0 \to 0] + \frac{p}{p+q} \cdot \Pr[1 \to 0]$$
$$= \frac{q}{p+q} \cdot (1-p) + \frac{p}{p+q} \cdot \frac{q}{p+q}$$
$$= \frac{q - pq + pq}{p+q} = \frac{q}{p+q} \quad \checkmark$$

$\therefore$ get to 1 w.p. $1 - \frac{q}{p+q} = \frac{p}{p+q}$. $\checkmark$

<u>Rem</u>: Given $-\boxed{A_x}-$, not easy to see what p, q are. So Nature is doing something powerful by setting σ according to $(*)$.

Could we take advantage of this?

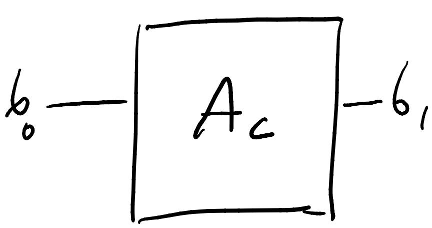
With 1 time-traveling bit, can efficiently solve CIRCUIT-SAT! (So can solve NP-complete problems. If you know complexity theory: can also solve coNP-complete probs.)

<u>Theorem</u>: BPP + 1 C.T.C. bit $\supseteq$ NP (and coNP)

(Results like this proven by Brun & Bacon, nailed down by Say & Yakaryılmaz, 2012. Exact power is known; it equals a weirdo class called BPP_{path} invented in 2001 in an algorithms paper about the stock market!)

<u>Proof</u>: Given C with n inputs, 1 output. Want to decide if it's satisfiable.

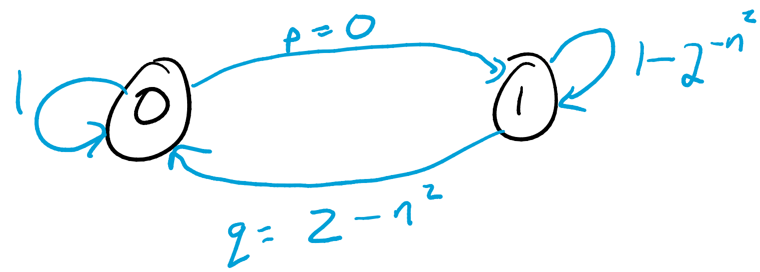
Make alg. (circuit) A_C:



"On input $b_0 \in \{0,1\}$,
Flip n^2 coins. If all heads, output $b_1 = 0$.
Else: pick $y \in \{0,1\}^n$ at random.
If $C(y) = 1$, output $b_1 = 1$.
Else output $b_1 = b_0$."

Case 1: C in unsatisfiable.

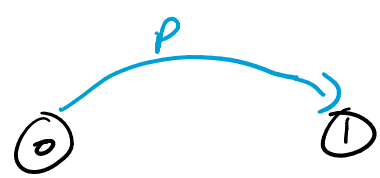
Then M.C. is...



Steady state: $\begin{cases} 0 \text{ with prob. } 100\% \\ 1 \quad \text{"} \quad \text{"} \quad 0\%. \end{cases}$

Case 2: C is satisfiable.

Then the



transition has

$$p \geq 2^{-n} - 2^{-n^2}$$

Pr[n^2 heads]

Pr[y is satisfying for C].

$$\Rightarrow \quad \frac{p}{p+q} \geq \frac{2^{-n} - 2^{-n^2}}{2^{-n}} \approx 1 - 2^{-n^2}$$

$\Rightarrow$ Steady state: $\begin{cases} 1 \text{ w. prob. } \approx 1 - 2^{-n^2} \\ 0 \text{ w. prob. } \approx 2^{-n^2}. \end{cases}$

So: as long as you put A_C in microwave, the incoming/outgoing bit tells you if C is satisfiable (except with teeny one-sided error)!

Also known:

- BPP + k CTC bits = "BPP_{path}" = BPP+1 CTC bit for any const. k (O'D.-Say '14)
- BQP + 1 CTC bit = PP (Aaronson '08)
  (Proof similar to Grover) (= BQP + k CTC bits, O'D-Say '15)

(Remark: Hard-core complexity theorists had long known that "PP ≠ BPP_{path} unless the polynomial hierarchy collapses". This gives another, time-travel-based proof, that classical computers can't simulate quantum ones unless PH collapses!)

- P or BPP or BQP or PSPACE + poly(n) CTC bits = PSPACE (Aaronson-Watrous '09)

(Poly time = poly space if time travel allowed! Proof is easy.)

These results assume you can send bits back in time by a poly(n) amount of time. What if you can only send them back O(1) time... but you can do this multiple times? (Say-Yakaryılmaz 2012)

- In this model all decidable L can be decided in expected time O(1)!

In conclusion...

1. From 1985 to 2020, Q.C. went from crazy theoretical dream to huge practical reality
2. The importance of fundamental/theory research: super-abstruse complexity theory from 30 years ago is crucially relevant to multi-million dollar Quantum Advantage experiments.
3. You now know more about Q.C. then most people... that work at Q.C. startups.
4. I think that the most exciting applications of Q.C.'s will be to solving <u>quantum</u> problems
5. Coming back to #1 ... time travel... hold on to your crazy dreams, they may become reality!