Title: Quantum Computation and the Foundations of Computational Complexity Theory

Date: Mar 28, 2017 03:30 PM

URL: http://pirsa.org/17030046

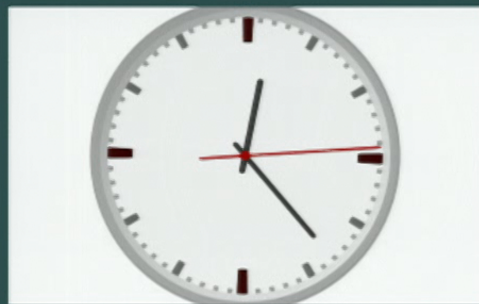
Abstract: <p>Computational complexity theory is a branch of computer science dedicated to classifying computational problems in terms of their difficulty. While computability theory tells us what we can compute in principle, complexity theory informs us regarding what is feasible. In this chapter I argue that the science of quantum computing illuminates the foundations of complexity theory by emphasising that its fundamental concepts are not model-independent. However this does not, as some have suggested, force us to radically revise the foundations of the theory. For model-independence never has been essential to those foundations. The fundamental aim of complexity theory is to describe what is achievable in practice under various models of computation for our various practical purposes. Reflecting on quantum computing illuminates complexity theory by reminding us of this, too often under-emphasised, fact.</p>

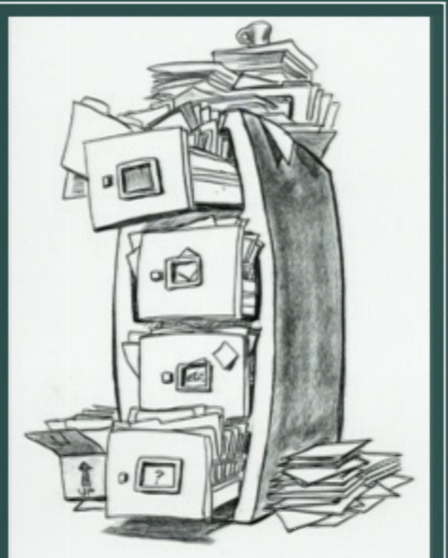
Quantum Computation and the Foundations of Computational Complexity Theory

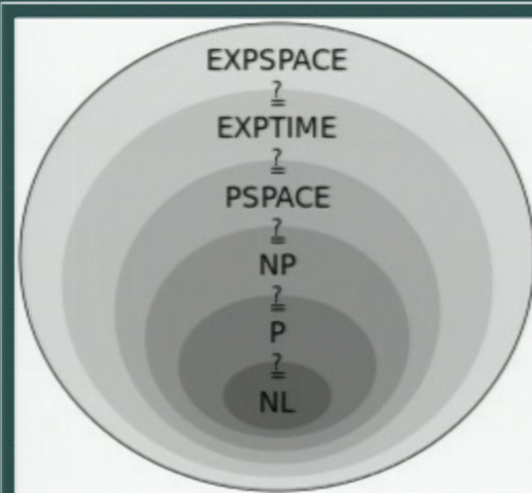
Michael Cuffaro, mcuffar@uwo.ca
Rotman Institute of Philosophy

Preprint available: http://philsci-archive.pitt.edu/12818/

Computability vs. Computational Complexity






EXPSPACE
?=
EXPTIME
?=
PSPACE
?=
NP
?=
P
?=
NL


French Advances / My Doctor Fired Me / Love App-tually
TIME
IT PROMISES TO SOLVE SOME OF HUMANITY'S MOST COMPLEX PROBLEMS. IT'S BACKED BY JEFF BEZOS, NASA AND THE CIA. EACH ONE COSTS $10,000,000 AND OPERATES AT 459° BELOW ZERO. AND NOBODY KNOWS HOW IT ACTUALLY WORKS
THE INFINITY MACHINE
BY LEV GROSSMAN

Consequences of quantum computing for complexity theory

Consequences of quantum computing for complexity theory

- "we must re-examine the foundations of computational complexity theory" (Bernstein and Vazirani 1997, p. 1412).
- "To my mind, the strongest implication is on the autonomous character of some of the theoretical entities used in computer science" (Hagar 2007, 244)

QC does not overturn the foundations of CCT.

CCT is a practical science.

- Model-independence is not a foundation for CCT.
- QC reminds us of this.

Consequences of quantum computing for complexity theory

- "we must re-examine the foundations of computational complexity theory" (Bernstein and Vazirani 1997, p. 1412).
- "To my mind, the strongest implication is on the autonomous character of some of the theoretical entities used in computer science" (Hagar 2007, 244)

QC does not overturn the foundations of CCT.

CCT is a practical science.

- Model-independence is not a foundation for CCT.
- QC reminds us of this.

Science does not (always) progress through the absolute identification of "fundamental entities."

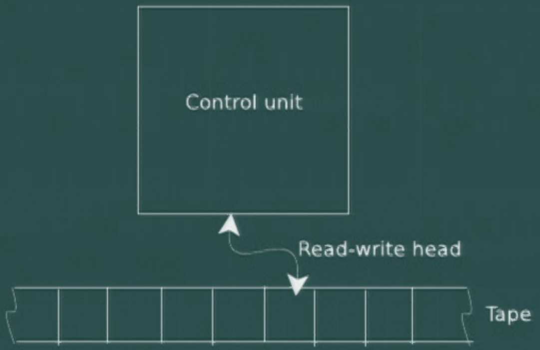
- Often built upon pragmatically justified foundations and conceptual structures.

Hilbert's programme

- Entscheidungsproblem (decision problem)

Hilbert's programme

- Entscheidungsproblem (decision problem)



Entscheidungsproblem:

- Find an effective method ...

Entscheidungsproblem:

- Find an effective method ...

Gödel 1956: "Dear Mr. von Neumann ..."

- $\varphi(n)$: steps needed (worst case) to decide if φ has a proof of length n.

14

Entscheidungsproblem:

- Find an effective method ...

Gödel 1956: "Dear Mr. von Neumann ..."

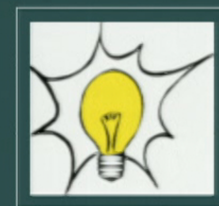
- $\varphi(n)$: steps needed (worst case) to decide if φ has a proof of length n.

$$\varphi(n) \propto n^2 \ ?$$

"... it would clearly indicate that, despite the unsolvability of the Entscheidungsproblem, the mental effort of the mathematician in the case of yes-or-no questions could be completely replaced by machines."

Computation

versus

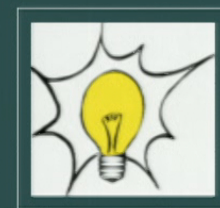


Ingenuity

$$\varphi(n) \propto n^2 \ ?$$

Computation

versus



Ingenuity

Irrelevant

$$\varphi(n) \propto n^2 \ ?$$

$\varphi(n) \propto n^2$: "small"

Modern complexity theory:

$$\varphi(n) \propto n^k: \text{ "small"}$$

Modern complexity theory:

$$\varphi(n) \propto n^k: \text{ “small”}$$

Solvable in a “small” (polynomial) number of steps:

- “efficiently solvable”
- “tractable”
- “feasible”
- “easy”
- etc.

Motivation: n^2 steps are "small".

```
mySubProcedure1(fanny) {
  // an efficient subroutine (requires a ''small'' number of steps)
}

mySubProcedure2(mae) {
  // an efficient subroutine (requires a ''small'' number of steps)
}

myProgram(fanny, mae) {
  mySubProcedure1(fanny);
  mySubProcedure2(mae);
}
```

Programmer's intuition: myProgram is also an efficient subroutine.

Motivation: n^2 steps are "small".

```
mySubProcedure1(fanny) {
  // an efficient subroutine (requires a ''small'' number of steps)
}

mySubProcedure2(mae) {
  // an efficient subroutine (requires a ''small'' number of steps)
}

myProgram(fanny, mae) {
  mySubProcedure1(fanny);
  mySubProcedure2(mae);
}
```

Programmer's intuition: myProgram is also an efficient subroutine.

Formally: closure under composition.

`mySubProcedure1` solvable in poly(n) steps.

`mySubProcedure2` solvable in poly(n) steps.

$\Rightarrow$ `myProgram` solvable in poly(n) steps.

P: $O(n^c)$ steps to compute with certainty

- Efficiently computable (deterministic TM)

P: $O(n^c)$ steps to compute with certainty

- Efficiently computable (deterministic TM)

NP: $O(n^c)$ steps to verify with certainty

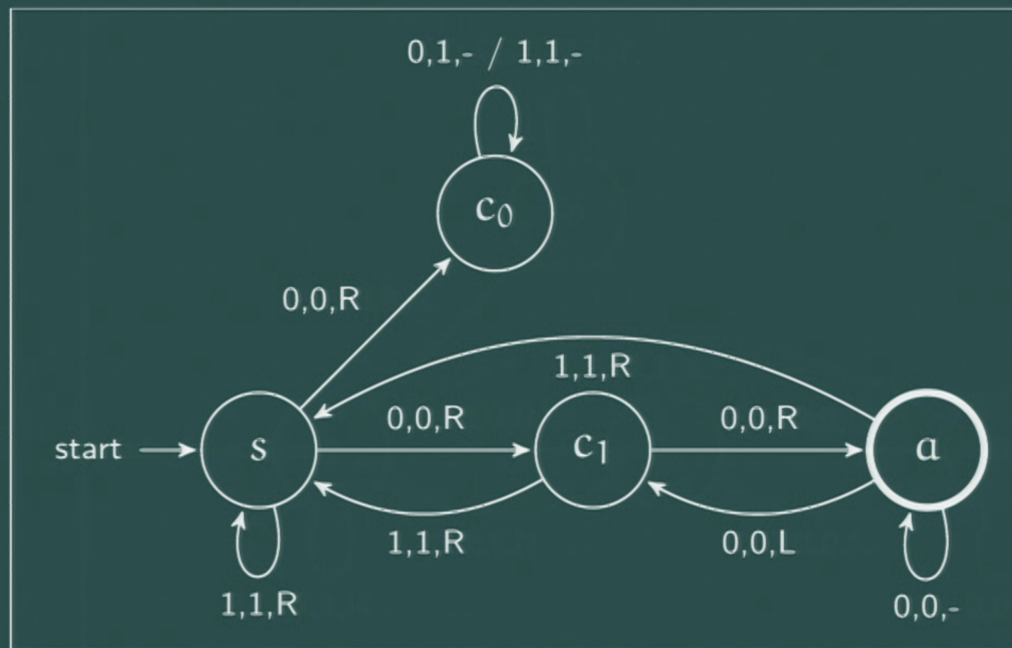
- Efficiently verifiable (deterministic TM)

P: $O(n^c)$ steps to compute with certainty

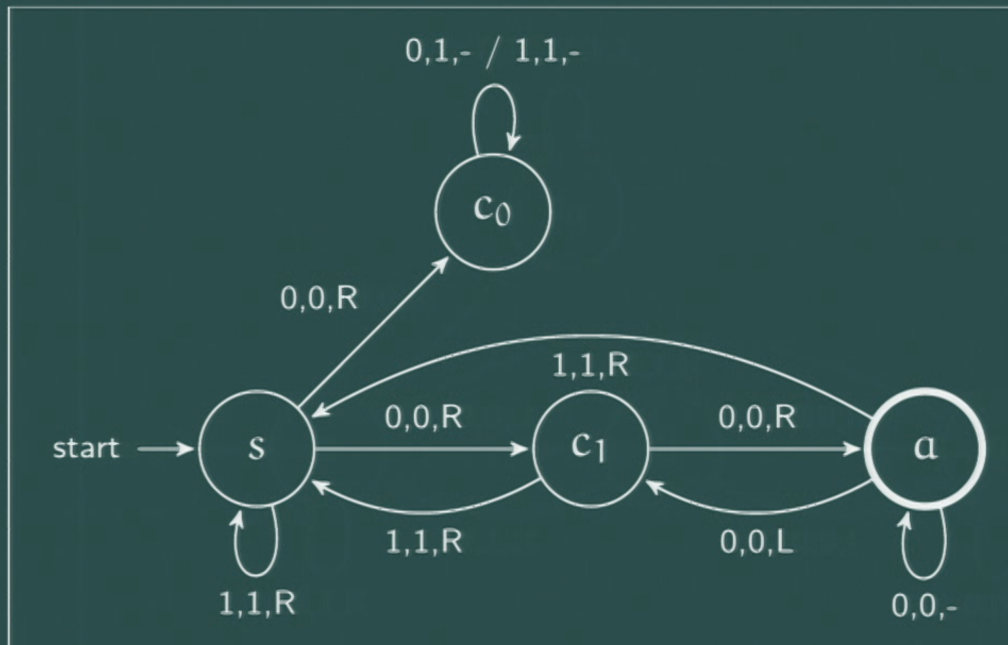
- Efficiently computable (deterministic TM)

NP: $O(n^c)$ steps to verify with certainty

- Efficiently verifiable (deterministic TM)
- Efficiently computable (nondeterministic TM)



Accepts: $*00$.



Accepts: $*00$.

P: $O(n^c)$ steps to compute with certainty

- Efficiently computable (deterministic TM)

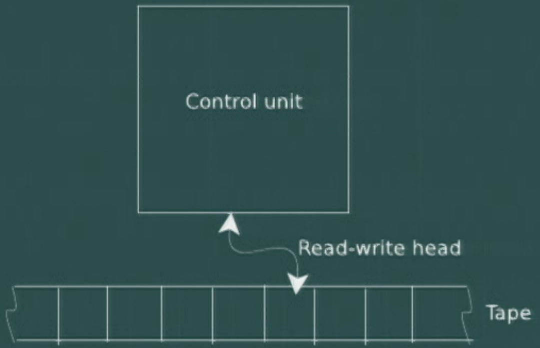
NP: $O(n^c)$ steps to verify with certainty

- Efficiently verifiable (deterministic TM)
- Efficiently computable (nondeterministic TM)

BPP: $O(n^c)$ steps to compute, with $\Pr_{\text{correct}} > 2/3$.

- Efficiently computable (probabilistic TM)

C-T thesis: p computable $\iff$ p computable by TM



C-T thesis: p computable $\iff$ p computable by TM

"Strong C-T thesis": p efficiently computable $\iff$ $\mathrm{p} \subseteq \mathbf{BPP}$

C-T thesis: $\mathfrak{p}$ computable $\iff$ $\mathfrak{p}$ computable by TM

Universality thesis: $\mathfrak{p}$ efficiently computable $\iff$ $\mathfrak{p} \subseteq \mathbf{BPP}$

$$\bigcup \mathsf{Poly}_{\mathfrak{M}} = \mathsf{BPP}.$$

C-T thesis: p computable $\iff$ p computable by TM

Universality thesis: p efficiently computable $\iff$ $\mathrm{p} \subseteq \mathbf{BPP}$

$$\bigcup \mathsf{Poly}_{\mathfrak{M}} = \mathsf{BPP}.$$

Invariance thesis: $\forall_{i,j}\ M_i \overset{\text{poly}}{\sim} M_j$

C-T thesis: p computable $\iff$ p computable by TM

Universality thesis: p efficiently computable $\iff$ $p \subseteq \mathbf{BPP}$

$$\bigcup \mathsf{Poly}_{\mathfrak{M}} = \mathsf{BPP}.$$

Invariance thesis: $\forall_{i,j}\ M_i \overset{\text{poly}}{\sim} M_j$

BQP: $O(n^c)$ steps to compute with a quantum computer, with $Pr_{\text{correct}} > 2/3$.

C-T thesis: p computable $\iff$ p computable by TM

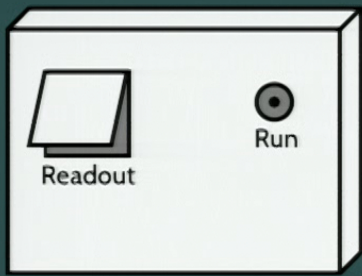
Universality thesis: p efficiently computable $\iff$ $p \subseteq \mathbf{BPP}$

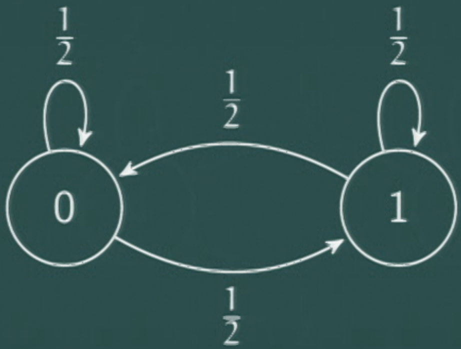
$$\bigcup \mathsf{Poly}_{\mathfrak{M}} = \mathsf{BPP}.$$

Invariance thesis: $\forall_{i,j}\ M_i \overset{\text{poly}}{\sim} M_j$

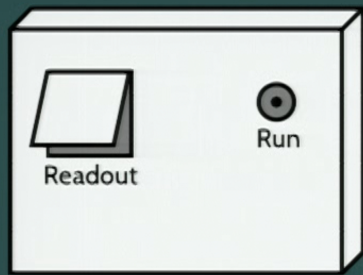
$\mathbf{BQP}$: $O(n^c)$ steps to compute with a quantum computer, with $Pr_{\text{correct}} > 2/3$.

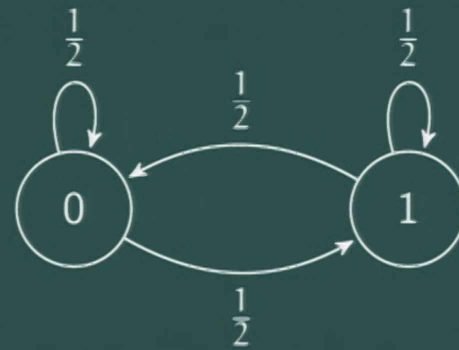
- $\mathbf{BPP} \subseteq \mathbf{BQP}$ ✓
- $\mathbf{BPP} \subsetneq \mathbf{BQP}$?



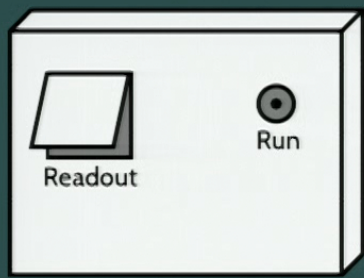


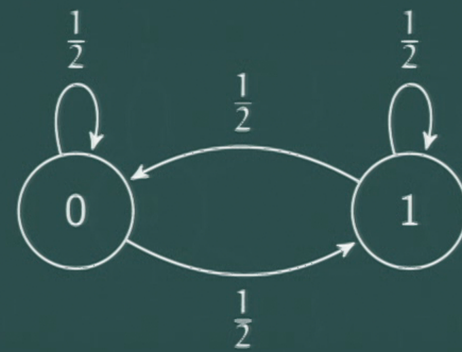
36





$\Pr(C0 \to 0)$

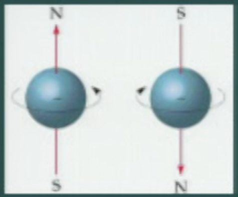




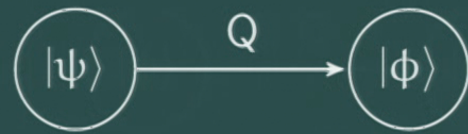
$$\Pr(C0 \to 0) = \Pr(C0 \to 1) = \Pr(C1 \to 0) = \Pr(C1 \to 1) = \tfrac{1}{2}$$

$$\begin{aligned}\Pr(C^2 0 \to 0) \;=\;& \Pr(C0 \to 0) \times \Pr(C0 \to 0) \\ &+ \Pr(C0 \to 1) \times \Pr(C1 \to 0) = \tfrac{1}{2}\end{aligned}$$

0, 1

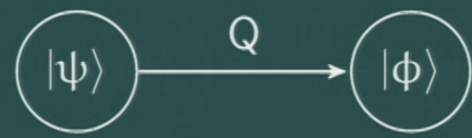


$|0\rangle, \ |1\rangle$



$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

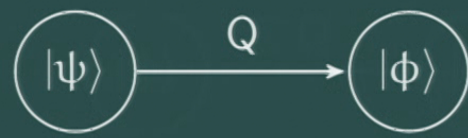
$|\phi\rangle = \delta|0\rangle + \gamma|1\rangle$



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad\qquad |\phi\rangle = \delta|0\rangle + \gamma|1\rangle$$

$$|0\rangle \xrightarrow{Q} \underbrace{\frac{i}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle}_{|\chi\rangle}$$

$$|1\rangle \xrightarrow{Q} \underbrace{\frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle}_{|\xi\rangle}$$

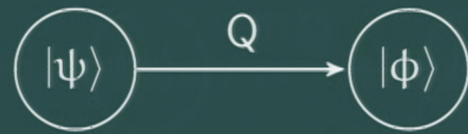


$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ $\qquad$ $|\phi\rangle = \delta|0\rangle + \gamma|1\rangle$

$$|0\rangle \xrightarrow{Q} \underbrace{\frac{i}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle}_{|\chi\rangle}$$

$$|1\rangle \xrightarrow{Q} \underbrace{\frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle}_{|\xi\rangle}$$

$$\Pr\left(|0\rangle \xrightarrow{\text{meas.}} 0\right) = |1|^2 = 1$$
$$\Pr\left(|\chi\rangle \xrightarrow{\text{meas.}} 0\right) = \left|\frac{i}{\sqrt{2}}\right|^2 = \frac{1}{2}$$

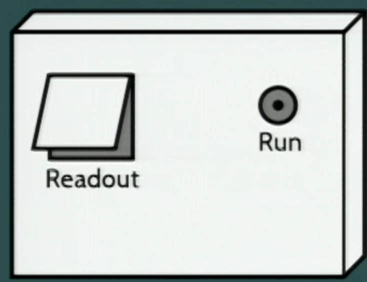


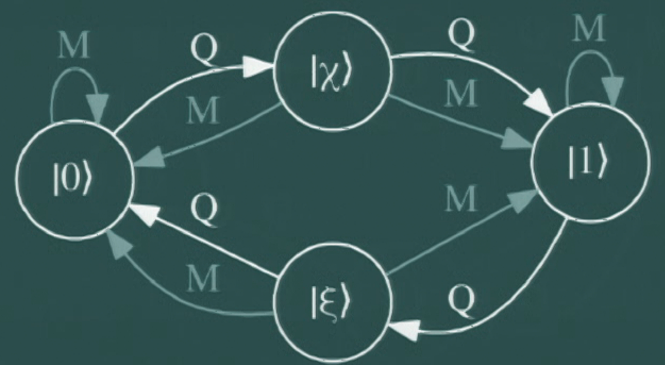
$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ $\qquad$ $|\phi\rangle = \delta|0\rangle + \gamma|1\rangle$

$$|0\rangle \xrightarrow{Q} \underbrace{\tfrac{i}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle}_{|\chi\rangle} \xrightarrow{Q} |1\rangle$$

$$|1\rangle \xrightarrow{Q} \underbrace{\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{i}{\sqrt{2}}|1\rangle}_{|\xi\rangle} \xrightarrow{Q} |0\rangle$$

$$\Pr\left(|0\rangle \xrightarrow{meas.} 0\right) = |1|^2 = 1$$
$$\Pr\left(|\chi\rangle \xrightarrow{meas.} 0\right) = \left|\tfrac{i}{\sqrt{2}}\right|^2 = \tfrac{1}{2}$$





$$|0\rangle \xrightarrow{Q} \underbrace{\frac{i}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle}_{|\chi\rangle} \xrightarrow{Q} |1\rangle$$

$$|1\rangle \xrightarrow{Q} \underbrace{\frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle}_{|\xi\rangle} \xrightarrow{Q} |0\rangle$$

$$\Pr(C0 \to 0) = \tfrac{1}{2}$$

$$\Pr(C0 \to 1) = \tfrac{1}{2}$$

$$\Pr(C1 \to 0) = \tfrac{1}{2}$$

$$\Pr(C1 \to 1) = \tfrac{1}{2}$$

$$\Pr(Q|0\rangle \xrightarrow{meas} 0) = \tfrac{1}{2}$$

$$\Pr(Q|0\rangle \xrightarrow{meas} 1) = \tfrac{1}{2}$$

$$\Pr(Q|1\rangle \xrightarrow{meas} 0) = \tfrac{1}{2}$$

$$\Pr(Q|1\rangle \xrightarrow{meas} 1) = \tfrac{1}{2}$$

48

$$\Pr(C0 \to 0) = \tfrac{1}{2} \qquad \Pr(Q|0\rangle \xrightarrow{meas} 0) = \tfrac{1}{2}$$

$$\Pr(C0 \to 1) = \tfrac{1}{2} \qquad \Pr(Q|0\rangle \xrightarrow{meas} 1) = \tfrac{1}{2}$$

$$\Pr(C1 \to 0) = \tfrac{1}{2} \qquad \Pr(Q|1\rangle \xrightarrow{meas} 0) = \tfrac{1}{2}$$

$$\Pr(C1 \to 1) = \tfrac{1}{2} \qquad \Pr(Q|1\rangle \xrightarrow{meas} 1) = \tfrac{1}{2}$$

$$\Pr(C^2 0 \to 0) = \tfrac{1}{2} \qquad \Pr(Q^2|0\rangle \xrightarrow{meas} 0) = 0$$

$$\Pr(C^2 0 \to 1) = \tfrac{1}{2} \qquad \Pr(Q^2|0\rangle \xrightarrow{meas} 1) = 1$$

$$\Pr(C^2 1 \to 0) = \tfrac{1}{2} \qquad \Pr(Q^2|1\rangle \xrightarrow{meas} 0) = 1$$

$$\Pr(C^2 1 \to 1) = \tfrac{1}{2} \qquad \Pr(Q^2|1\rangle \xrightarrow{meas} 1) = 0$$


French Advances / My Doctor Fired Me / Love App-tually
TIME
IT PROMISES TO SOLVE SOME OF HUMANITY'S MOST COMPLEX PROBLEMS. IT'S BACKED BY JEFF BEZOS, NASA AND THE CIA. EACH ONE COSTS $10,000,000 AND OPERATES AT 459° BELOW ZERO. AND NOBODY KNOWS HOW IT ACTUALLY WORKS
THE INFINITY MACHINE
BY LEV GROSSMAN

Gödel 1956: "Dear Mr. von Neumann ..."

$\varphi(n)$: steps needed (worst case) to decide if φ has a proof of length n.

"... it would clearly indicate that, despite the unsolvability of the Entscheidungsproblem, the mental effort of the mathematician in the case of yes-or-no questions could be completely replaced by machines."

$$\varphi(n) \propto n^k \ ?$$

$$\mathsf{P} \stackrel{?}{=} \mathsf{NP}$$

$\mathbf{BPP} \subseteq \mathbf{BQP}$

$\mathbf{BPP} \subsetneq \mathbf{BQP}$?

Indirect evidence:

- Shor's algorithm
- Oracle results
- etc.

Universality thesis:

Any 'reasonable' model of computation can be efficiently simulated on a probabilistic Turing machine (Bernstein & Vazirani 1997, 1411).

- p efficiently computable $\Longleftrightarrow$ $\mathrm{p} \subseteq \mathbf{BPP}$

54

(Hagar 2007, 244-5):

"To my mind, the strongest implication is on the autonomous character of some of the theoretical entities used in computer science ... given that quantum computers may be able to efficiently solve classically intractable problems, hence redescribe the space of computational complexity, computational concepts and even computational kinds such as 'an efficient algorithm' or 'the class NP', will become machine-dependent, and recourse to 'hardware' will become inevitable in any analysis of the notion of computational complexity."

Further implications:

- Cognitive science, philosophy of mind, etc.

Universality thesis:

Any 'reasonable' model of computation can be efficiently simulated on a probabilistic Turing machine (Bernstein & Vazirani 1997, 1411).

- Model independence?

[The truth of the universality thesis would be] great news for the theory of computational complexity, for it implies that attention may be restricted to the probabilistic Turing machine model of computation. After all, if a problem has no polynomial resource solution on a probabilistic Turing machine, then the [universality of Turing efficiency] implies that it has no efficient solution on any computing device. Thus, the [universality of Turing efficiency] implies that the entire theory of computational complexity will take on an elegant, model-independent form if the notion of efficiency is identified with polynomial resource algorithms (Nielsen & Chuang, p. 140).

$$\bigcup \mathsf{Poly}_{\mathfrak{M}} = \mathsf{BPP}.$$

p_1 is efficiently solvable under model M_A.
p_2 is efficiently solvable under model M_B.
p_3 is efficiently solvable under model M_C.
p_4 is efficiently solvable under model M_D.
...

Universal (Randomised) Turing Machine

vs.

Universal Quantum Computer

$$\bigcup \mathrm{Poly}_{\mathfrak{M}} = \mathrm{BPP}.$$

vs

$$\bigcup \mathrm{Poly}_{\mathfrak{M}} = \mathrm{BQP}.$$

Invariance thesis

$$\forall_{i,j}\ M_i \overset{\text{poly}}{\sim} M_j$$

63

The fundamental complexity classes P and NP became part of a fundamental hierarchy: LOGSPACE, NLOGSPACE, P, NP, PSPACE, EXPTIME, ... And again theory faced the problem that each of these classes has a machine-dependent definition, and that efficient simulations are needed before one can claim that these classes are in fact machine-independent and represent fundamental concepts of computational complexity. It seems therefore that complexity theory, as we know it today, is based on the [assumption that the invariance thesis holds] (van Emde Boas 1990, p. 5).

LOGSPACE, NLOGSPACE, P, NP, PSPACE, EXPTIME, ...

- Classes of languages
- $L_{primes} = \{10, 11, 101, 111, 1011, 1101, 10001, 10011, \ldots\}$
- $L_{primes} \in P$

LOGSPACE, NLOGSPACE, P, NP, PSPACE, EXPTIME, ...

- Classes of languages
- $L_{primes} = \{10, 11, 101, 111, 1011, 1101, 10001, 10011, \ldots\}$
- $L_{primes} \in P$

$P \stackrel{?}{=} NP$

Gödel 1956: "Dear Mr. von Neumann ..."

By no means does computational complexity "rest upon" a [universality of Turing efficiency] thesis. The goals [sic.] of computational complexity is to consider different notions of efficient computation and compare the relative strengths of these models. Quantum computing does not break the computational complexity paradigm but rather fits nicely within it. (Fortnow, 2006).

$O(n^c)$: polynomial $\Rightarrow$ 'efficient'

$O(n^c)$: polynomial $\Rightarrow$ 'efficient'

- n^{1000} vs. $2^{n/1000}$

$O(n^c)$: polynomial $\Rightarrow$ 'efficient'

- n^{1000} vs. $2^{n/1000}$

Of the big problems solvable in polynomial time—matching, linear programming, primality testing, etc.—most of them really do have practical algorithms. And of the big problems that we think take exponential time—theorem-proving, circuit minimization, etc.—most of them really don't have practical algorithms. So, that's the empirical skeleton holding up our fat and muscle. (Aaronson 2013, p. 54).

The goal of computational complexity theory.

- Model-independent characterisation of efficient computation?
- 'Practical' science
    - Normative character
    - Model-independence inessential

Invariance thesis

$$\forall_{i,j}\ M_i \overset{\text{poly}}{\sim} M_j$$

~~Invariance thesis~~

~~$$\forall_{i,j}\ M_i^{R} \overset{\text{poly}}{\sim} M_j^{R}$$~~

$$\forall_{i,j}\ M_i^{C} \overset{\text{poly}}{\sim} M_j^{C}$$

$$\forall_{i,j}\ M_i^{Q} \overset{\text{poly}}{\sim} M_j^{Q}$$

Invariance principle

74

~~Invariance thesis~~

~~$$\forall_{i,j}\ M_i^{R} \overset{poly}{\sim} M_j^{R}$$~~

$$\forall_{i,j}\ M_i^{C} \overset{poly}{\sim} M_j^{C}$$

$$\forall_{i,j}\ M_i^{Q} \overset{poly}{\sim} M_j^{Q}$$

Invariance principle

~~Invariance thesis~~

$$\sout{\forall_{i,j}\ M_i^{R} \overset{poly}{\sim} M_j^{R}}$$

$$\forall_{i,j}\ M_i^{C} \overset{poly}{\sim} M_j^{C}$$

$$\forall_{i,j}\ M_i^{Q} \overset{poly}{\sim} M_j^{Q}$$

Invariance principle

- Methodological principle
  - organising
  - simplifying
  - relative model-independence

The goal of computational complexity theory.

- Model-independent characterisation of efficient computation?
- 'Practical' science
    - Normative character
    - Model-independence inessential

Does quantum computing break the paradigm of computational complexity theory?

- No.
- It reminds us of the point of it all.