CS480/CS580 QUANTUM COMPUTING

Lecture 1: Introduction

GENERAL INFORMATION

Instructor: Özlem Salehi Köken

E-mail: ozlem.koken@ozyegin.edu.tr

Office: EF103

Office Hours: Wednesday 14:30-16:30

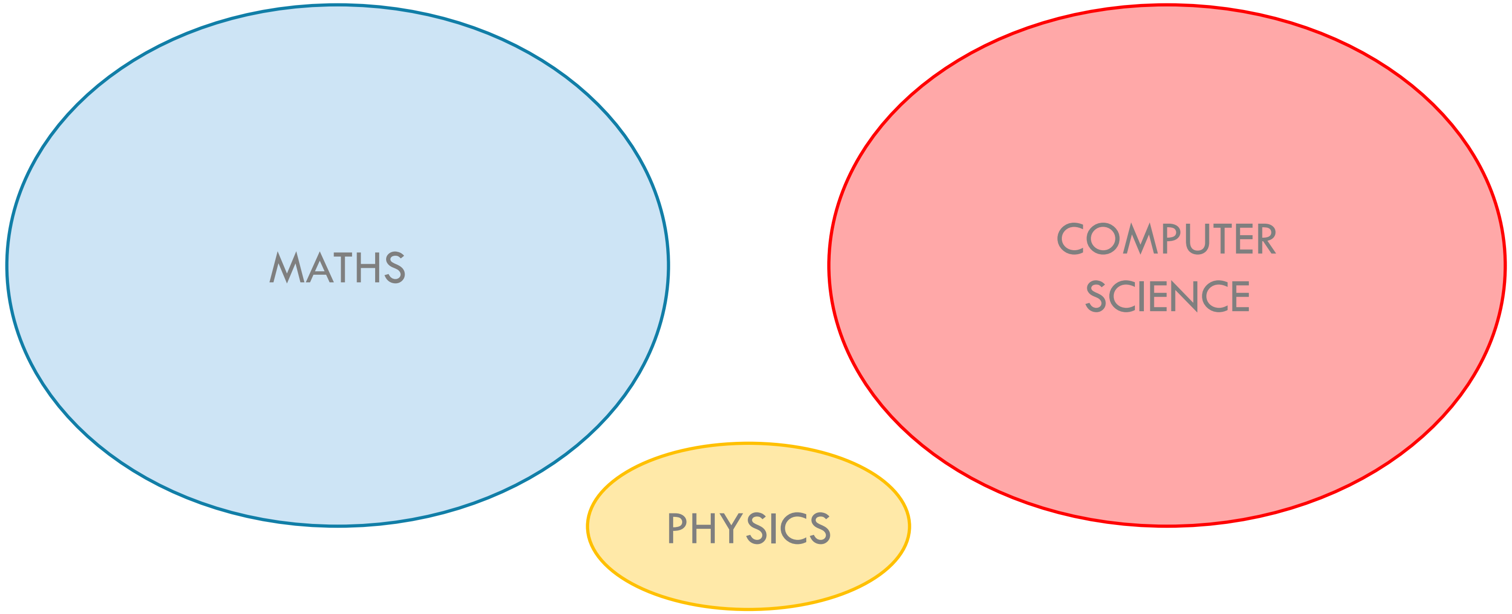
Books: Michael Nielsen, Isaac Chuang - Quantum Computation and Quantum Information

Suggested: David Mermin - Quantum Computer Science

Kaye, Laflamme, Mosca - An Introduction to Quantum Computing

Scott Aaronson - Quantum Computing Since Democritus

COURSE CONTENT



COURSE CONTENT

- Computational models, Church-Turing Thesis, History of quantum computing, Extended Church-Turing thesis
- Complexity theory, deterministic and probabilistic systems, mathematical background
- Basics of quantum systems, quantum circuit model, gates, superposition, measurement
- Entanglement, Superdense coding, teleportation
- Quantum computational complexity, query complexity, phase kickback
- Deutsch-Jozsa Algorithm, Bernstein-Vazirani Algorithm
- Simon's algorithm, Grover's Search Algorithm
- Quantum Fourier Transform, Shor's algorithm
- Quantum Key Distribution
- Quantum finite automata and Quantum Turing machine

GRADING

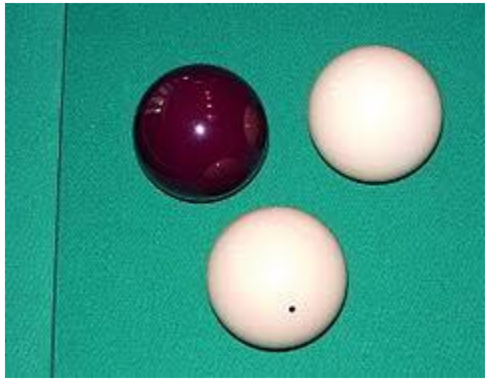
CS480

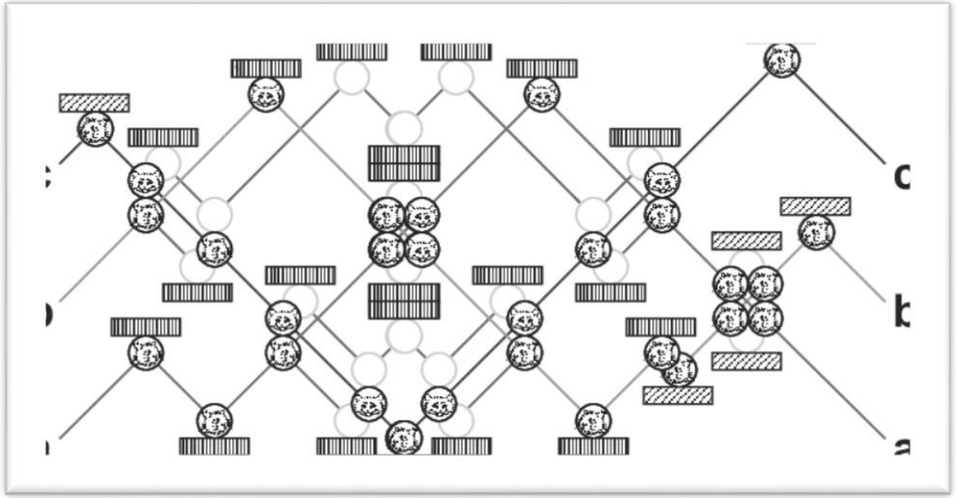
- Midterm %30
- Final %40
- Homework %30

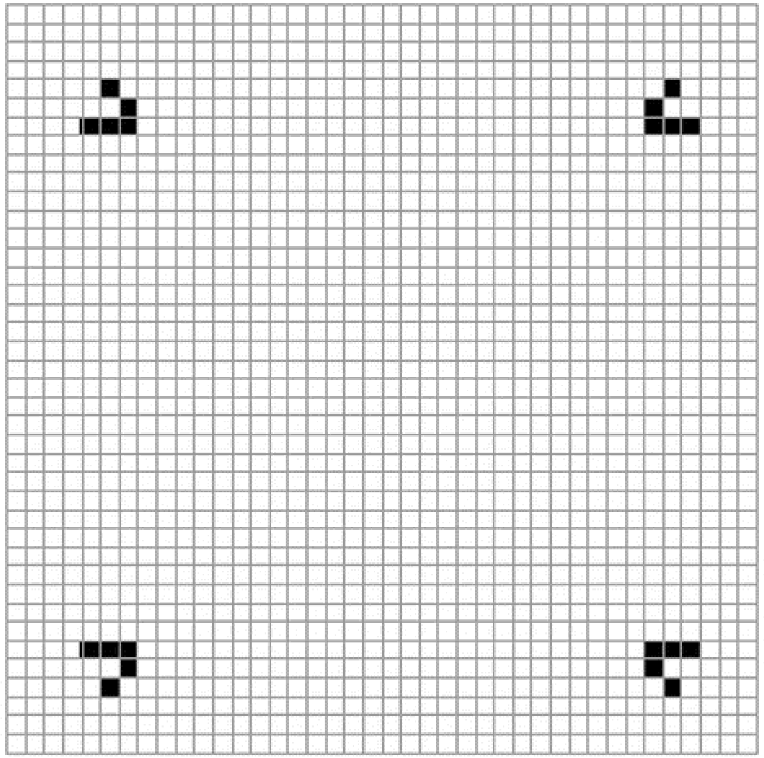
CS580

- Midterm %25
- Final %35
- Homework %20
- Report %10
- Presentation %10

MODELS OF COMPUTATION

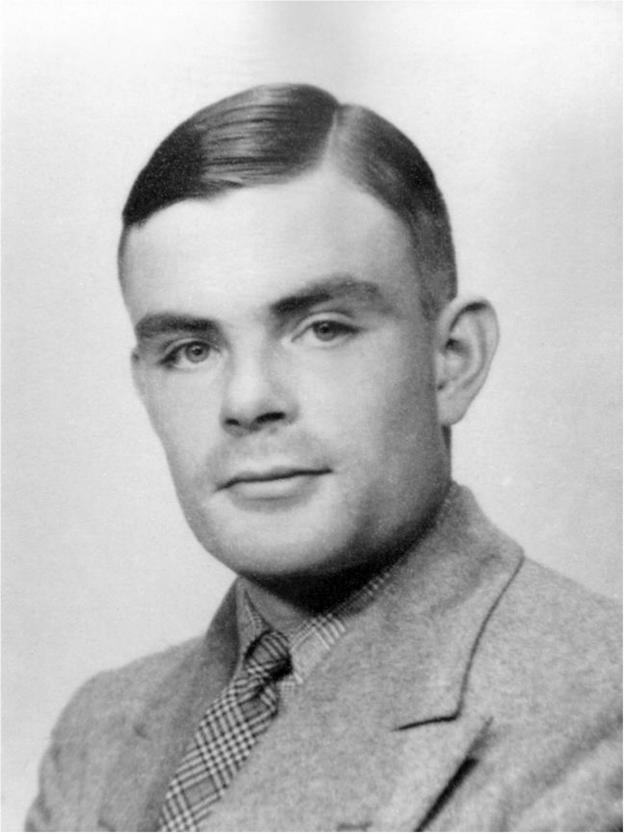


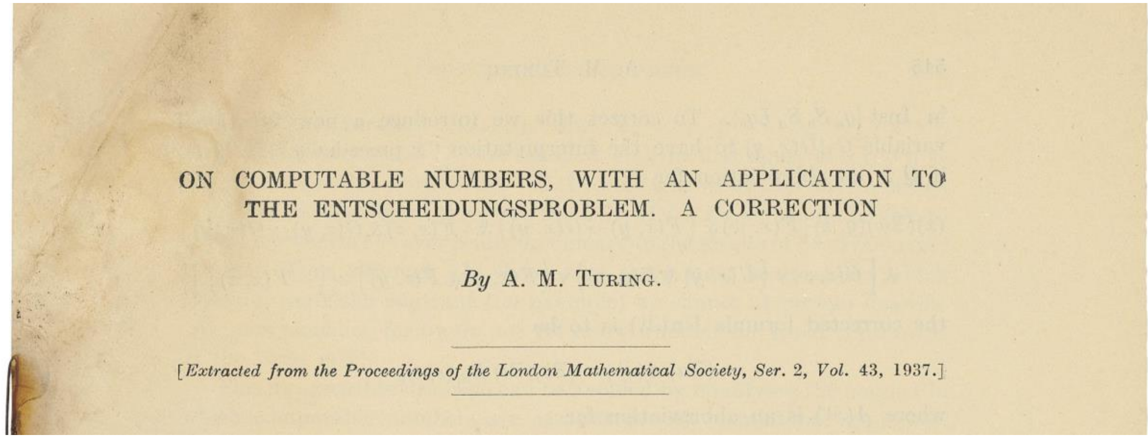




Fredkin, Edward; Toffoli, Tommaso (1982), "Conservative logic", International Journal of Theoretical Physics, **21** (3–4): 219–253
https://jeremykun.com/2011/06/29/conways-game-of-life/

ALAN TURING (1912-1954)



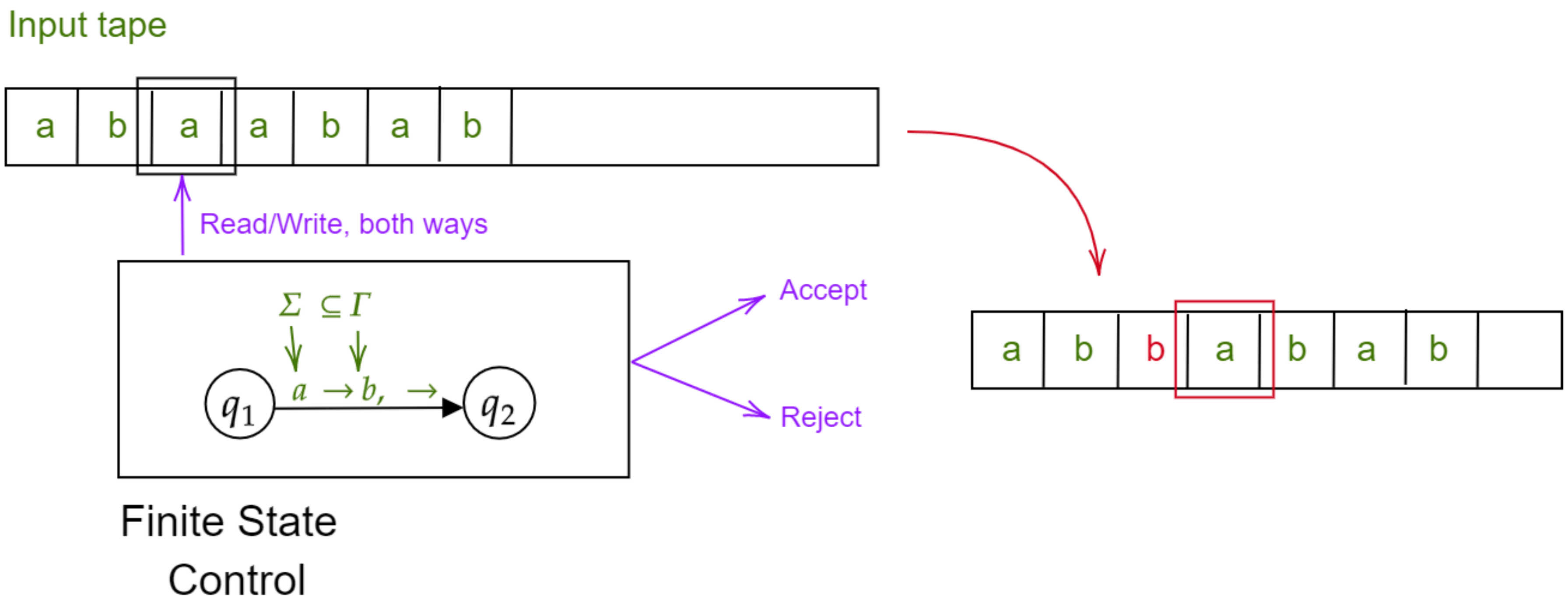

ON COMPUTABLE NUMBERS, WITH AN APPLICATION TO THE ENTSCHEIDUNGSPROBLEM. A CORRECTION

By A. M. TURING.

[*Extracted from the Proceedings of the London Mathematical Society, Ser.* 2, *Vol.* 43, 1937.]

Birth of computer science

TURING MACHINE



$$\mathbf{P} = \cup_{c \geq 1} \mathbf{DTIME}(n^c)$$

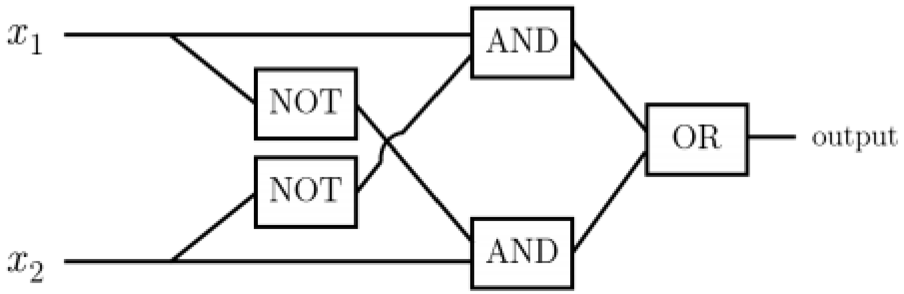
$$\mathbf{NP} = \cup_{c \geq 1} \mathbf{NTIME}(n^c)$$

CHURCH-TURING THESIS

"Every function which would naturally be regarded as computable can be computed by the universal Turing machine."

- All possible formalizations of the intuitive mathematical notion of algorithm or computation are equivalent to each other

BOOLEAN CIRCUITS

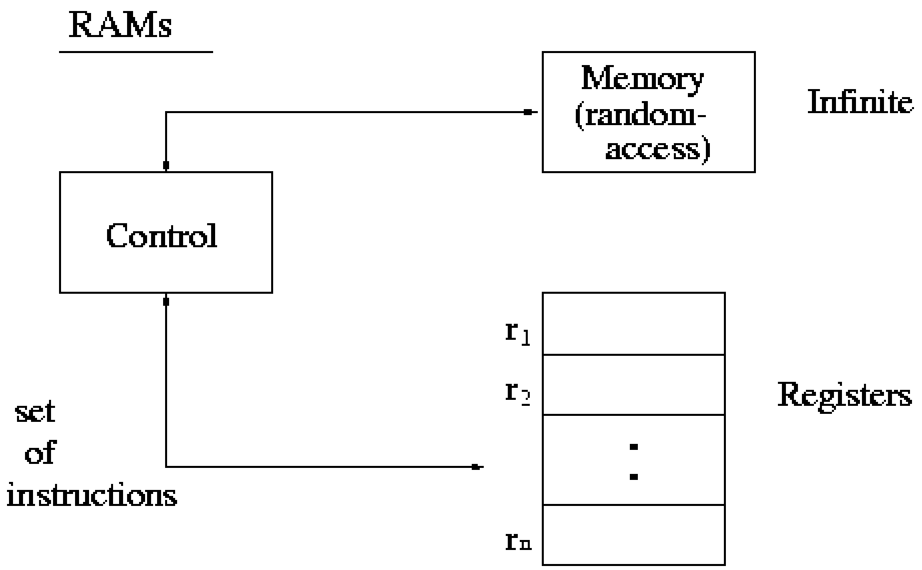


Any Boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ is computable by a Boolean circuit C using just *AND*, *OR*, and *NOT* gates. i.e., *AND*, *OR*, and *NOT* gates are universal.

A language L is computable by a **P***-uniform circuit family iff L* ∈ **P.**

https://www.cs.cmu.edu/~odonnell/quantum15/QuantumComputationScribeNotesByRyanODonnellAndJohnWright.pdf

RANDOM ACCESS MACHINE



https://grid.cs.gsu.edu/~cscskp/Automata/propTM/node10.html

EXTENDED CHURCH-TURING THESIS

"Every physically realizable computation model can be simulated by a TM with polynomial overhead."

Simulation of one model by another is *efficient* if the 'overhead' in resources used by the simulation is *polynomial* (i.e. simulating an $O(f(n))$ algorithm uses $O(f(n)^k)$ resources for some fixed integer k).

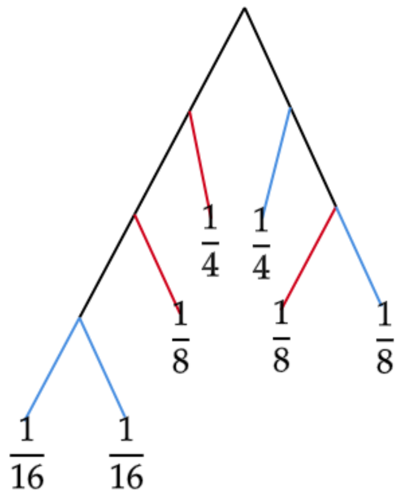
Does probabilistic computation violate «Extended Church-Turing Thesis»?

PROBABILISTIC TURING MACHINE

- TM + coin flip
- At each step flip a coin and branch into two with probability ½
- We consider deciders only: probabilities sum upto 1
- Runtime: Worst case over all branches
- Bounded error computation (ε can be any value between (0 , ½))

  If $w \in L$, $P(M \text{ accepts } w) \geq 1 - \varepsilon$

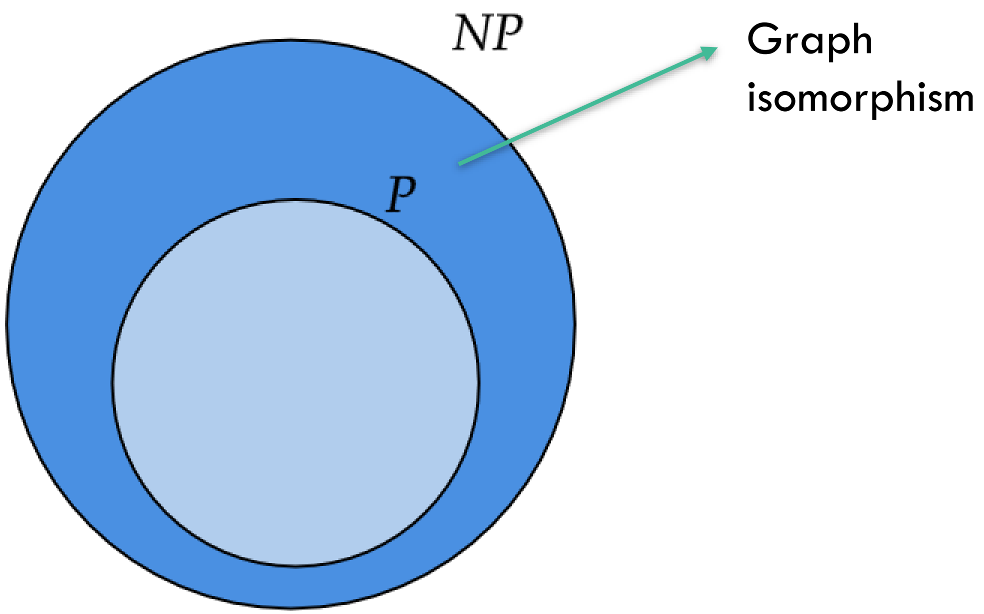
  If $w \notin L$, $P(M \text{ rejects } w)\ ) \geq 1 - \varepsilon$

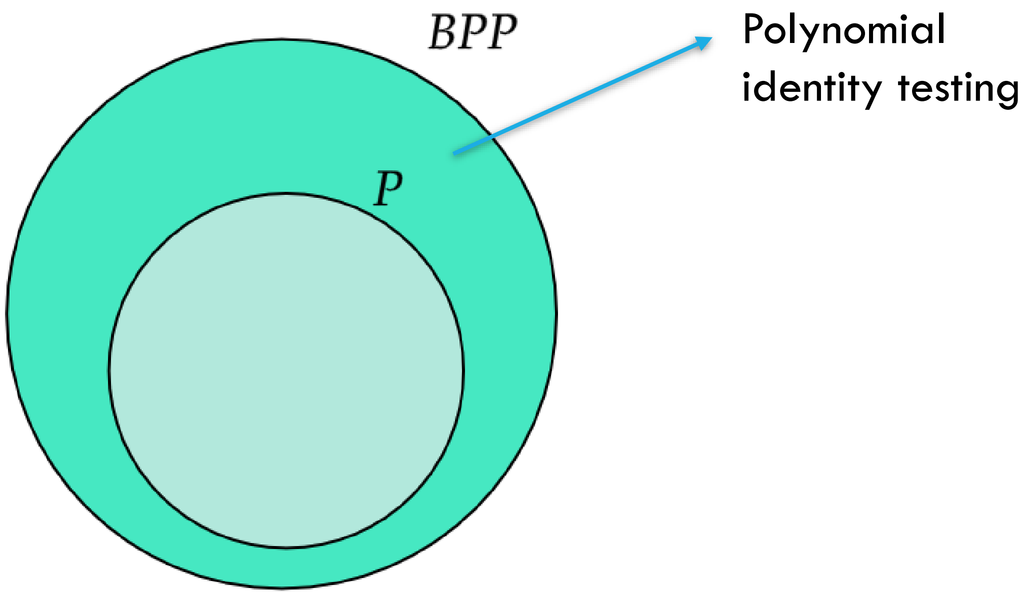


BPP A language is in BPP if there exists a probabilistic Turing Machine deciding L with error probability $\varepsilon = 1/3$

P VS NP VS BPP VS EXP

- $P \subseteq NP \subseteq EXP$ P vs. NP ?
- $P \subseteq BPP \subseteq EXP$ P vs. BPP ?





It is strongly believed that $P \neq NP$ and $P = BPP$

BACK TO EXTENDED CHURCH-TURING THESIS

Does probabilistic computation violate «Extended Church-Turing Thesis»?

It is «believed» that the answer is no and Extended Church-Turing Thesis is sometimes stated as

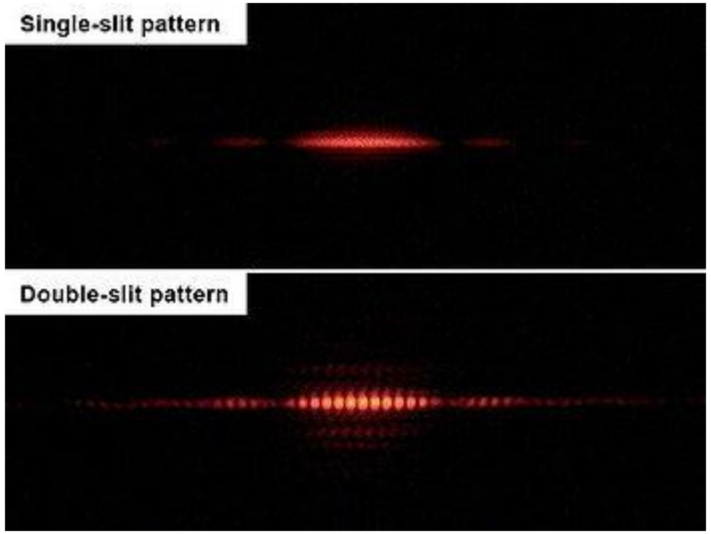
"Every physically realizable computation model can be simulated by a **probabilistic** TM with polynomial overhead."

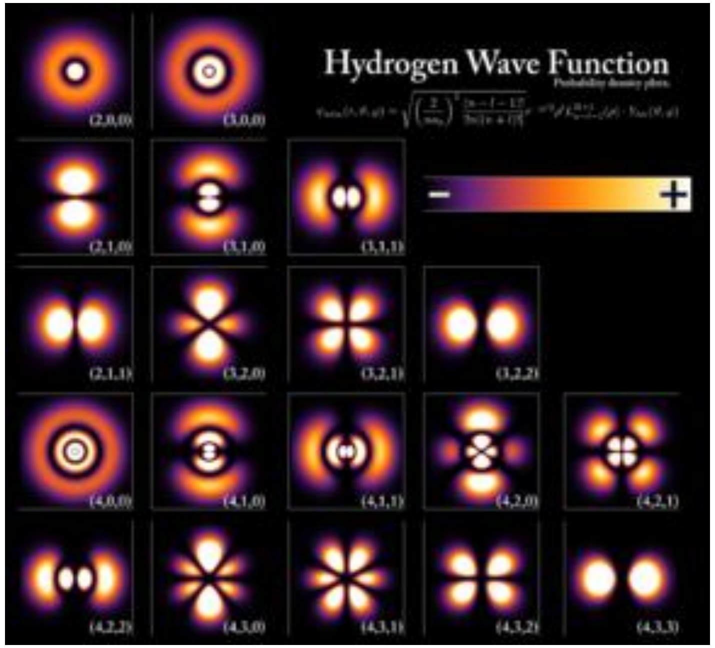
Does quantum computation violate «Extended Church-Turing Thesis»?

QUANTUM COMPUTING

QUANTUM COMPUTING

- Quantum Computing is the use of quantum-mechanical phenomena such as superposition and entanglement to perform computation.



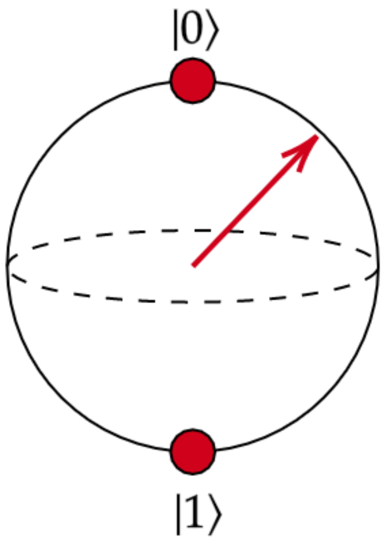


https://en.wikipedia.org/wiki/Quantum_computing

AMPLITUDES AND MEASUREMENT

- To fully describe the state of an isolated system, you need to give one amplitude for each possible configuration that you could find the system in on measuring it.
- Probabilities are the squared absolute values of the amplitudes
- Different Interpretations
  - Niels Bohr (Copenhagen interpretation
  - Hugh Everett (Many worlds interpretation)
  - David Bohm (Non-local hidden variables)

BIT VS QUBIT



Physical support	$\|0\rangle$	$\|1\rangle$
Photon	Horizontal	Vertical
	Vacuum	Single photon state
	Early	Late
Coherent state of light	Amplitude-squeezed state	Phase-squeezed state
Electrons	Up	Down
	No electron	One electron
Nucleus	Up	Down
Optical lattices	Up	Down
Josephson junction	Uncharged superconducting island (Q=0)	Charged superconducting island (Q=2e, c
	Clockwise current	Counterclockwise current
	Ground state	First excited state
Singly charged quantum dot pair	Electron on left dot	Electron on right dot
Quantum dot	Down	Up
Gapped topological system	Depends on specific topological system	Depends on specific topological system
van der Waals heterostructure[10]	Electron on bottom sheet	Electron on top sheet

https://en.wikipedia.org/wiki/Qubit

MODELS OF QUANTUM COMPUTING

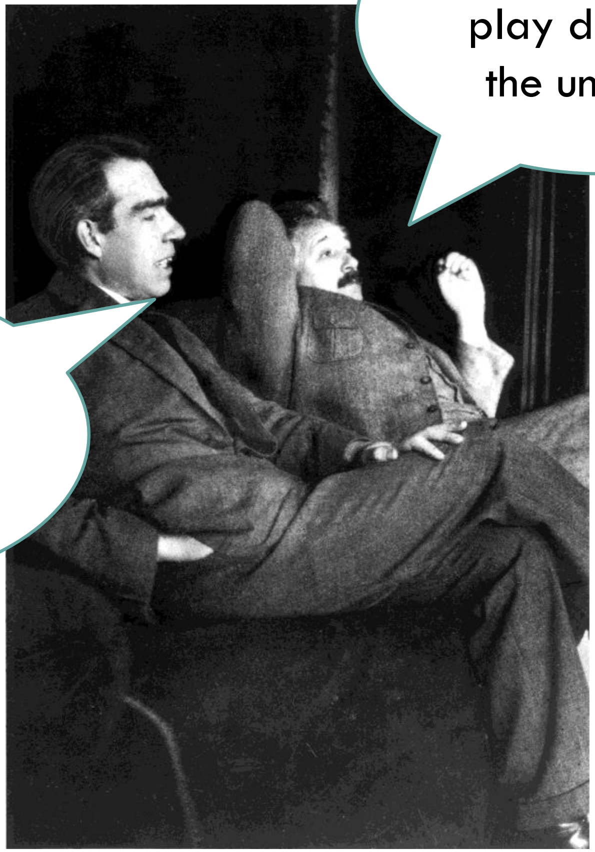
- Quantum simulation
- Quantum annealing
- Adiabatic quantum computation
- Trapped ion quantum computing
- Superconducting quantum computing
- Quantum Turing Machine
- Quantum Circuit Model

A BRIEF HISTORY OF QUANTUM COMPUTING

- 1927 – Solvay Conference

15 out of 27 in this photo won the Nobel Prize.

https://www.epiqc.cs.uchicago.edu/qc-history



A BRIEF HISTORY OF QUANTUM COMPUTING

- 1980 – Benioff

  Simulated a Turing machine with an abstract model working under the laws of quantum mechanics

- 1981 – Feynman

  Idea of simulating nature by quantum computers

RICHARD FEYNMAN (1918-1988)

Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981

NATURE ISN'T CLASSICAL, DAMMIT, AND IF YOU WANT TO MAKE A SIMULATION OF NATURE, YOU'D BETTER MAKE IT QUANTUM MECHANICAL, AND BY GOLLY IT'S A WONDERFUL PROBLEM, BECAUSE IT DOESN'T LOOK SO EASY.

A BRIEF HISTORY OF QUANTUM COMPUTING

- 1984 – Richard Feynman

    Basis of quantum mechanical computer using reversible gates

    It seems that the laws of physics present no barrier to reducing the size of computers until bits are the size of atoms, and quantum behavior holds dominant sway.

- 1985 – David Deutsch

    Universal quantum computer – Church-Turing-Deutsch Principle

DAVID DEUTSCH (1953 -)

Proc. R. Soc. Lond. A **400**, 97–117 (1985)
Printed in Great Britain

Quantum theory, the Church–Turing principle and the universal quantum computer

By D. Deutsch
Department of Astrophysics, South Parks Road, Oxford OX1 3RQ, U.K.

(*Communicated by R. Penrose, F.R.S. – Received* 13 *July* 1984)

Birth of quantum computing

CHURCH-TURING-DEUTSCH PRINCIPLE

Church-Turing Thesis

"Every function which would naturally be regarded as computable can be computed by the universal Turing machine."

- All possible formalizations of the intuitive mathematical notion of algorithm or computation are equivalent to each other

Church-Turing-Deutsch Principle

"**Every finitely realizable physical system** can be perfectly simulated by a universal model computing machine operating by finite means"

- functions which would naturally be regarded as computable ~ in principle be computed by a real physical system

http://michaelnielsen.org/blog/interesting-problems-the-church-turing-deutsch-principle/

A BRIEF HISTORY OF QUANTUM COMPUTING

- 1992 – Deustch Jozsa Algorithm
  First example of exponential speedup against any deterministic algorithm (relative to oracle)
- 1992 – Bernstein-Vazirani Problem
- 1994 – Simon's Problem
  Exponential speedup over any probabilistic algorithm (relative to oracle)
- 1994 – Shor's Algorithm
  Factoring prime numbers – Polynomial time algorithm
  Exponentially faster than the most efficient known classical algorithm
- 1996 – Grover's Search Algorithm
  Quadratic speedup for searching

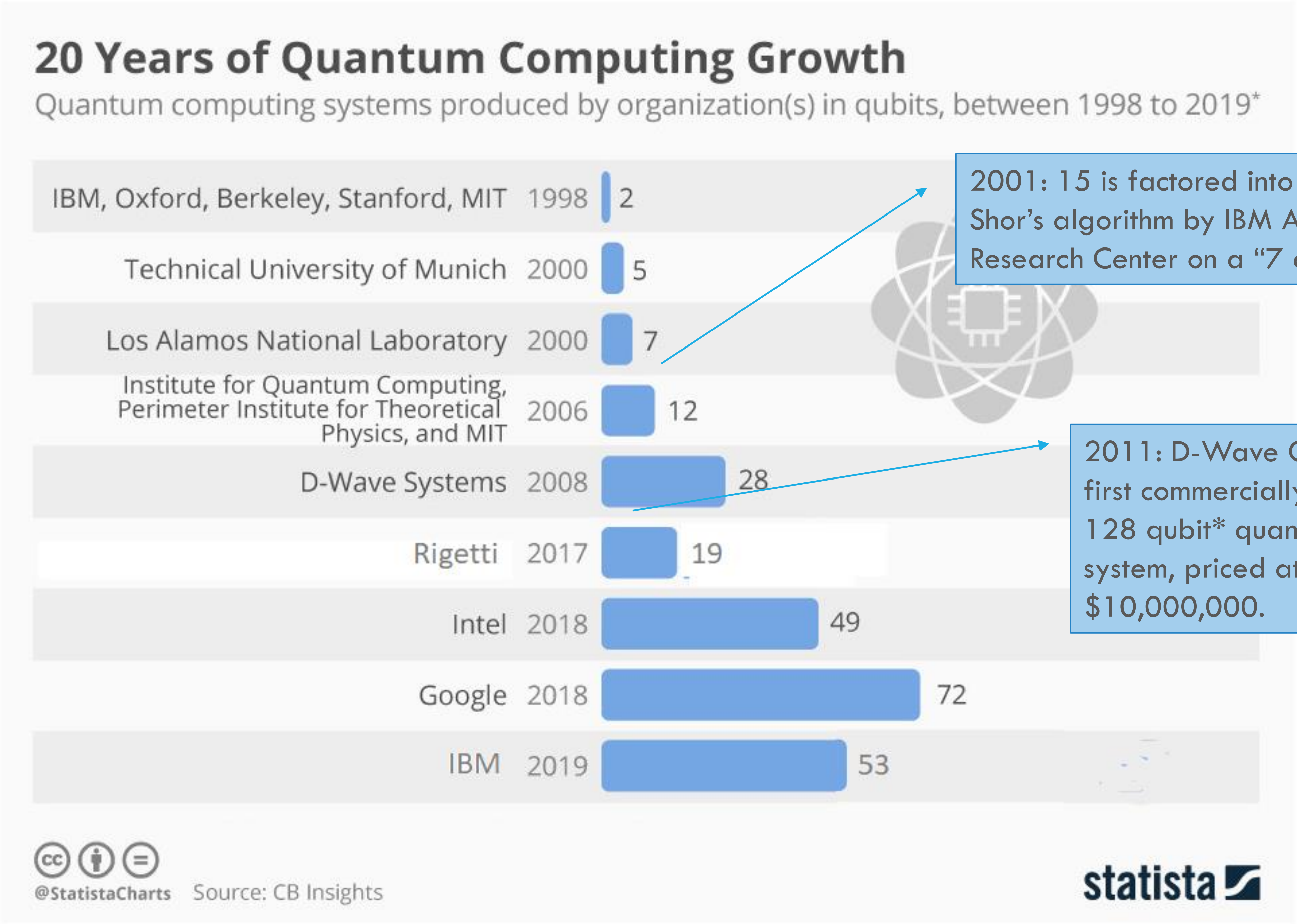
BACK TO EXTENDED CHURCH-TURING THESIS

Does quantum computation violate «Extended Church-Turing Thesis»?

It is believed that the answer is **yes.**

Does quantum computation violate «Church-Turing Thesis»?

No since quantum computers can be simulated by ordinary Turing machines.



2001: 15 is factored into 5 and 3 using Shor's algorithm by IBM Almaden Research Center on a "7 qubit computer"

2011: D-Wave One, world's first commercially available 128 qubit* quantum computer system, priced at $10,000,000.

QUANTUM SUPREMACY

- Solving a problem by a quantum computer that is not practically solvable by a classical computer

nature

Article | Published: 23 October 2019

Quantum supremacy using a programmable superconducting processor

Frank Arute, Kunal Arya, [...] John M. Martinis

Nature **574**, 505–510(2019) | Cite this article

Quantum technologies + Add to myFT

Google claims to have reached quantum supremacy

Researchers say their quantum computer has calculated an impossible problem for ordinary machines

Madhumita Murgia and **Richard Waters** SEPTEMBER 20 2019

Google and IBM Clash Over Milestone Quantum Computing Experiment

21

Today Google announced that it achieved "quantum supremacy." Its chief quantum computing rival, IBM, said it hasn't. The disagreement hinges on what the term really means.

IBM

IBM Research Blog Topics Labs About

October 21, 2019 | Written by: Edwin Pednault, John Gunnels & Dmitri Maslov, and Jay Gambetta

Categorized: Quantum Computing

October 29, 2018

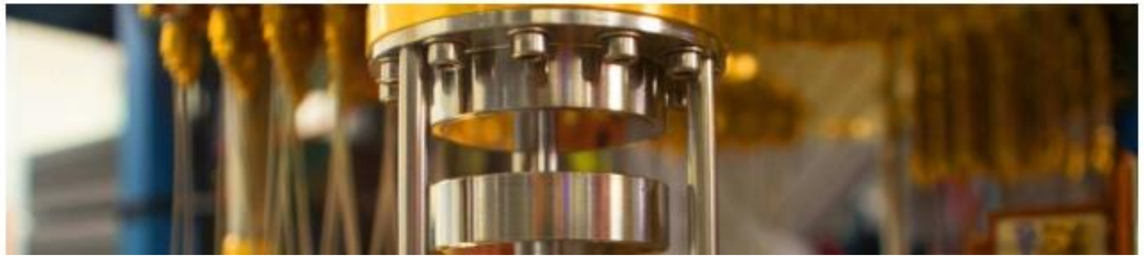
 | Oct 10, 2019, 03:37pm

Quantum USA Vs. Quantum China: The World's Most Important Technology Race

Moor Insights and Strategy Contributor
Cloud
Straight talk from Moor Insights & Strategy tech industry analysts

Computing Dec 22, 2018

President Trump has signed a $1.2 billion law to boost US quantum tech



India finally commits to quantum computing, promises $1.12B investment

by IVAN MEHTA — 8 days ago in INDIA

WHAT'S NEXT?

- Mathematical background, from classical systems to quantum systems, vector notation
- Quantum circuit model, quantum gates
- Basic protocols and algorithms