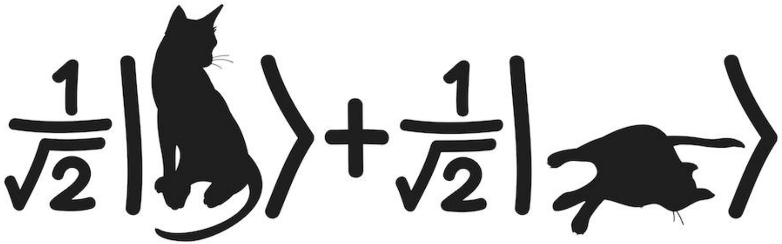
Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley



Lecture 16: Quantum Complexity Theory

BQP and Extended Church-Turing Thesis

Computational problems:

e.g. multiply matrices M, N.

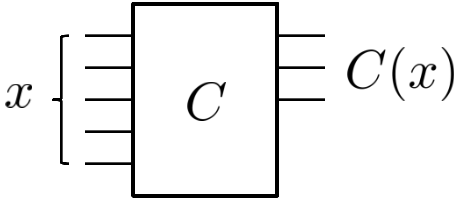
test whether N is prime

write N as a product of prime factors.

is the boolean formula f(x) satisfiable?

A polynomial time algorithm is one that on inputs of size n, halts in time O(n^k) for some constant k, and outputs the answer.

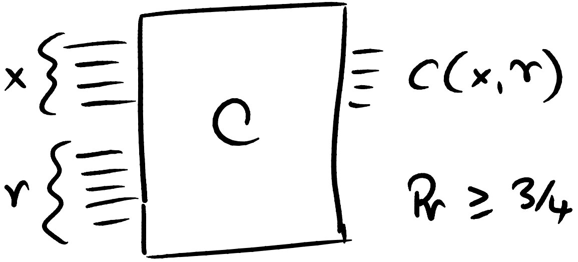
running time ≡ size of C



A polynomial time algorithm is one that on inputs of size n, halts in time O(n^k) for some constant k, and outputs the answer.

The class P or polynomial time, is the class of all computational problems with polynomial time algorithms.

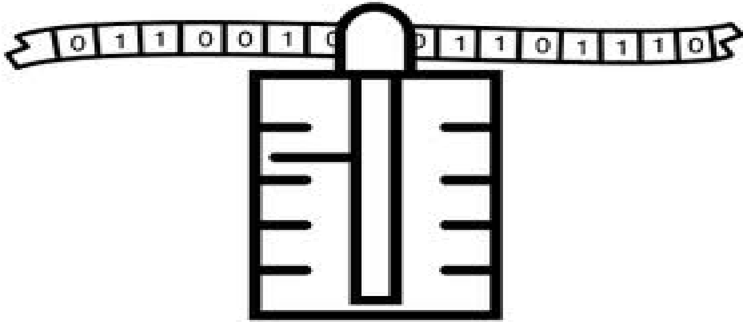
The class BPP, or bounded error probabilistic polynomial time, is the class of computational problems which have polynomial time randomized algorithms that output the correct answer with high probability.



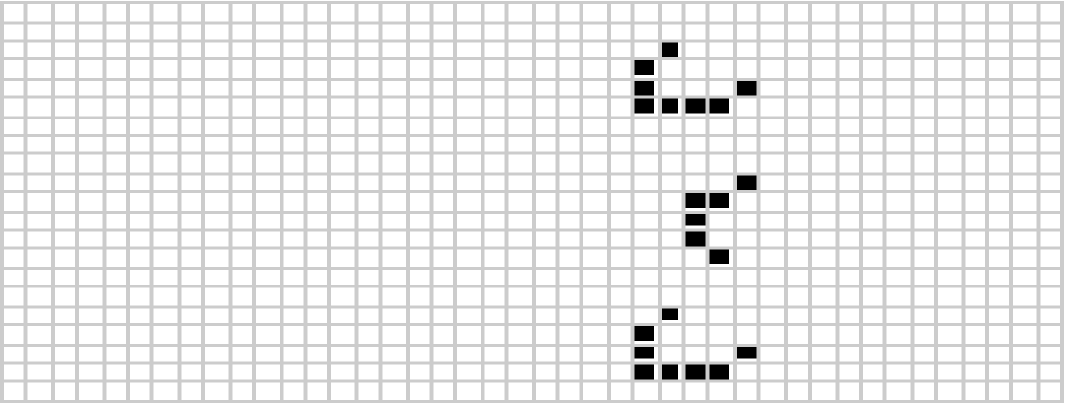
Polynomial time good,
Exponential time bad!!

Extended Church–Turing Thesis

Any “reasonable” model of computation can be simulated on a (probabilistic) Turing Machine with at most polynomial simulation overhead. T steps → $O(T^2)$

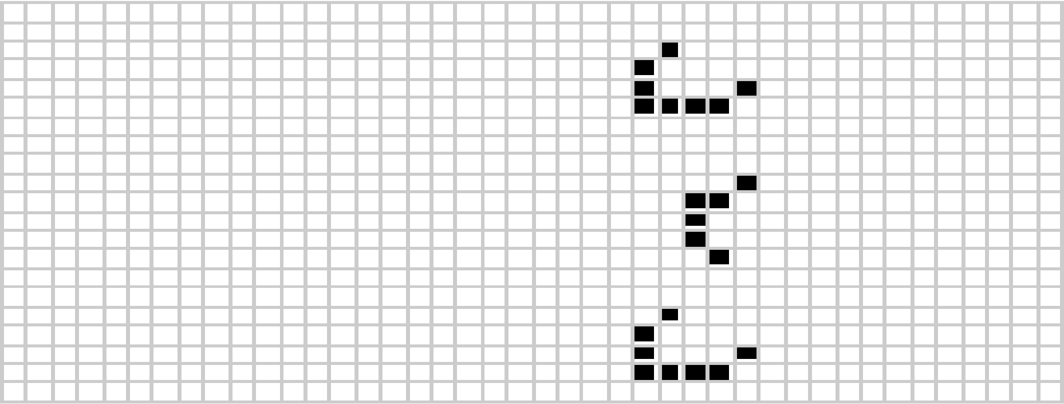


- Turing Machine describes the set of functions that are humanly computable. i.e the class P describes what you could compute with an unlimited amount of pape at your disposal.



- The class P represents what can be physically computed.

Nature as a Computer



Classical physics — local differential equations

Cellular automata discretization of LDE. ⊙

digital abstraction.

Quantum computation is the only model of computation that violates the Extended Church–Turing thesis.

Evidence:

Black box separations:
Recursive fourier sampling
Simon’s problem.

Breaks cryptography:
Factoring
Discrete logs

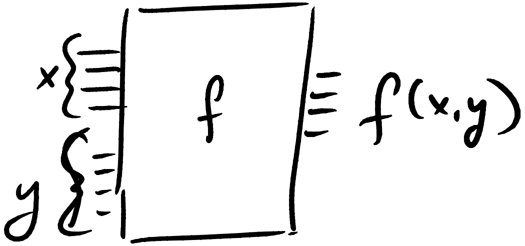
Why can’t we prove an unconditional result?

The class BQP, or bounded error ~~probabilistic~~ quantum polynomial time, is the class of computational problems which have polynomial time quantum algorithms that output the correct answer with high probability.

$$P \subseteq BPP \subseteq BQP \subseteq P^{\#P} \subseteq PSPACE$$

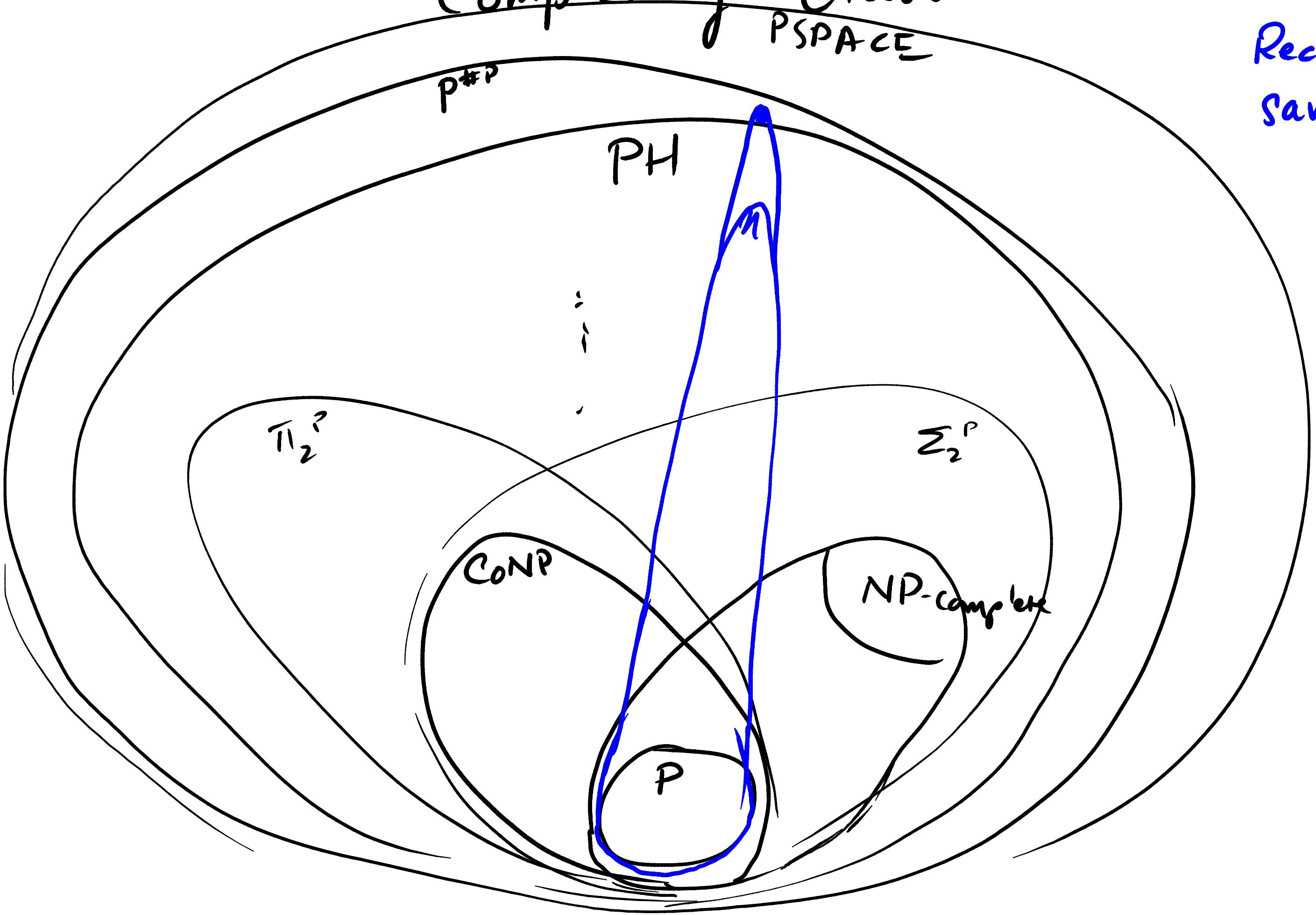
P vs PSPACE   Open Question

#P   countig class.



$$C(x) = \sum_{y} f(x,y)$$

Complexity Classes.



Recursive fourier sampling : ∉ MA

Black box or oracle model

Could BQP contain problems much outside NP?

BQP vs PH: central open question in quantum complexity.

Conjecture (1993): Fourier sampling ∉ PH

New conjecture: [Aaronson 09] Fourier checking ∉ PH
http://www.scottaaronson.com/papers/bqpph.pdf

$$\begin{pmatrix} \\ v_k \\ \\ \\ \end{pmatrix}$$

v, w random unit vectors in R^N $N = 2^n$
Distinguish f = sgn(v) & g = sgn(Hv) from f = sgn(v) & g = sgn(w)
Where f,g:$\{0,1\}^n \to \{1,-1\}$

$K \to sgn(K)$