P vs NP

A DESPERATE SEARCH

BY SANDOR DALECKE

P vs NP

A DESPERATE SEARCH

BY SANDOR DALECKE

IS THERE A DIFFERENCE BETWEEN CHECKING A PROOF AND FINDING ONE?

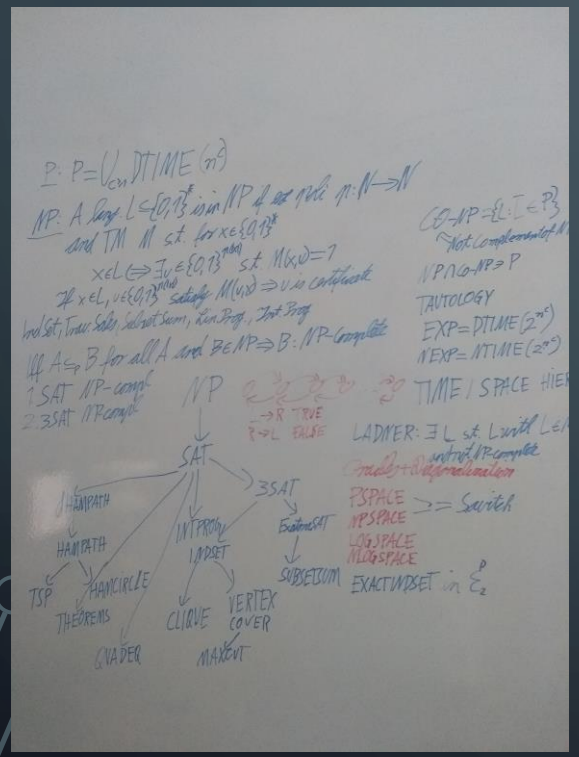
SOME BASICS

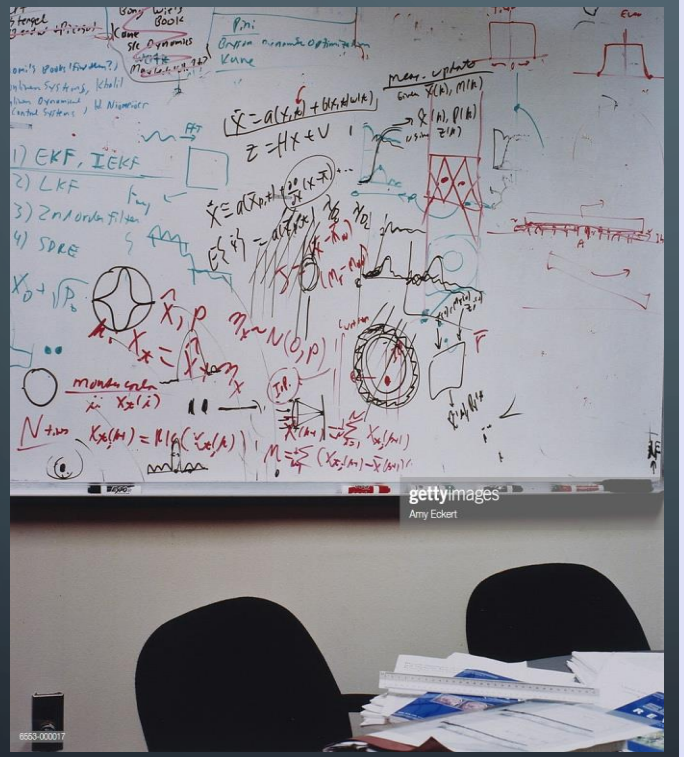
- **P** is the class of problems solvable by a Turing machine in polynomial time
  - Sort a list:
    - Bubblesort is in $O(n^2)$ → P 300^2 = 90 000
- **NP** is the class of problems for which, if the answer is yes, then there's a polynomial-size *proof* of that fact that you can *check* in polynomial time.
  - SAT (Check if a Boolean formula is TRUE):
    - Checking one solution is easy
    - Finding a solution? Best we know is Brute Force O(2^n) 2^300 = ?

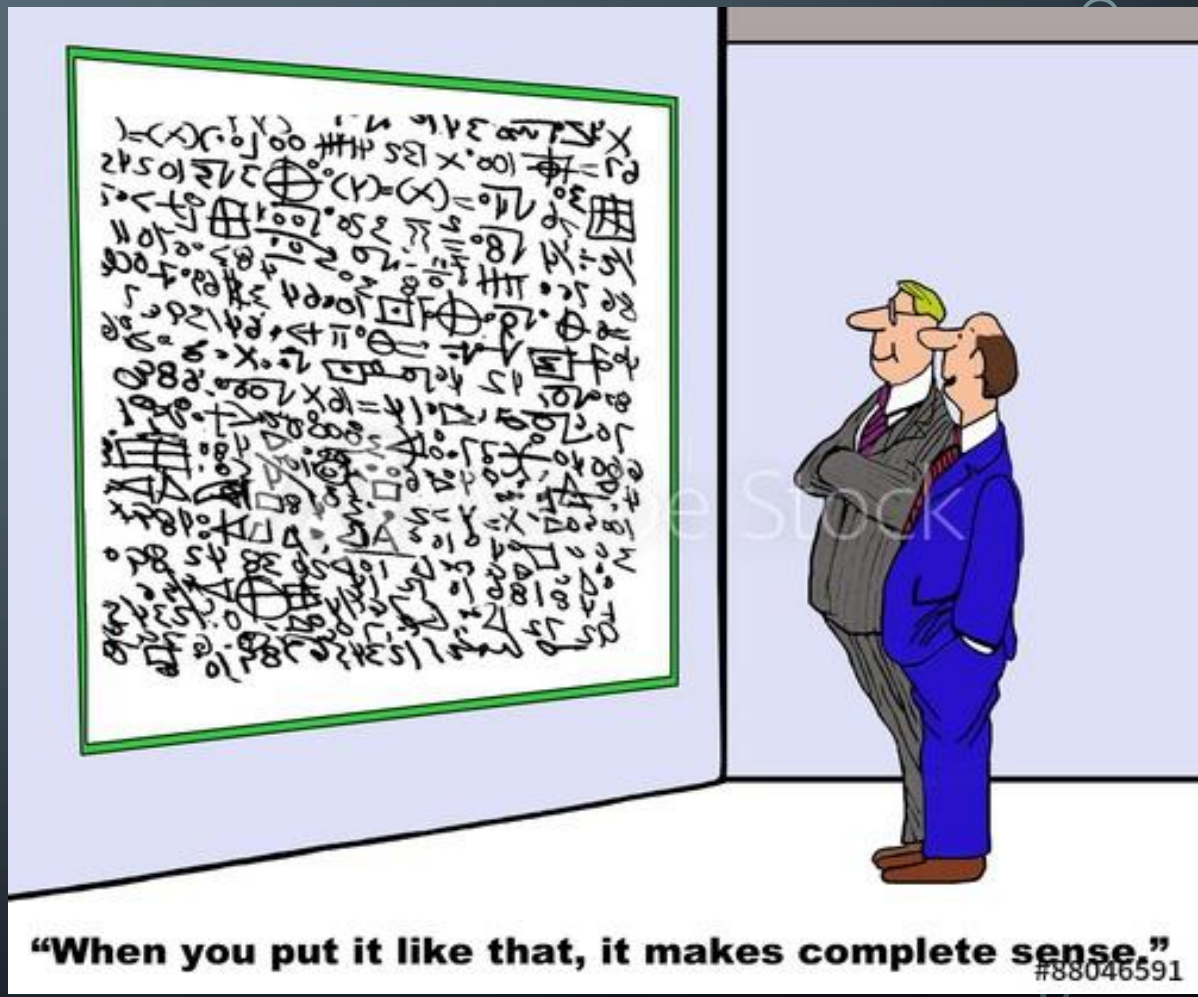
WHY DO WE CARE?

- If P = NP:
  - Fold Proteins ✓
  - Break most cryptography ✓
  - Packing Boxes perfectly ✓
  - Always find the best travel route ✓
  - Always find the shortest prove for every theorem ✓

LET‘S PROVE THIS: USE MATH!

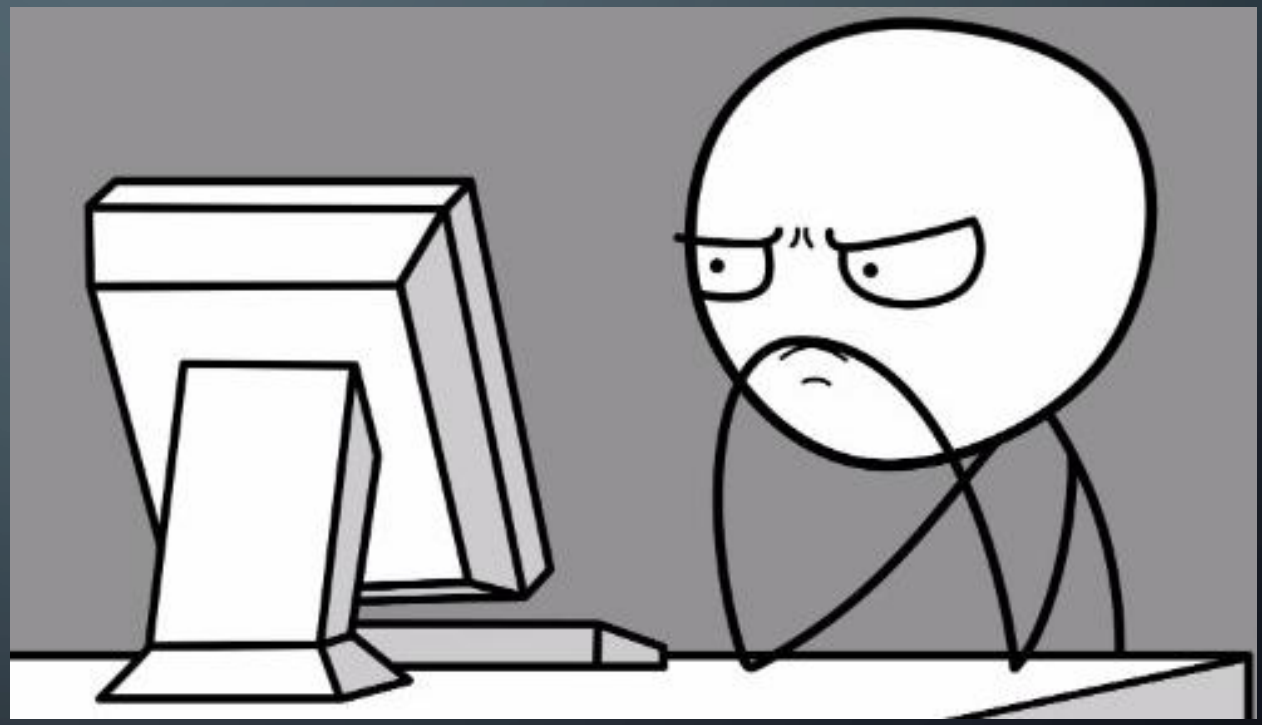






METHOD: COMPLEMENT

- P = Co-P
- SATISFIABILITY vs TAUTOLOGY
- IF NP ≠ Co-NP → P ≠ NP
- We don‘t know

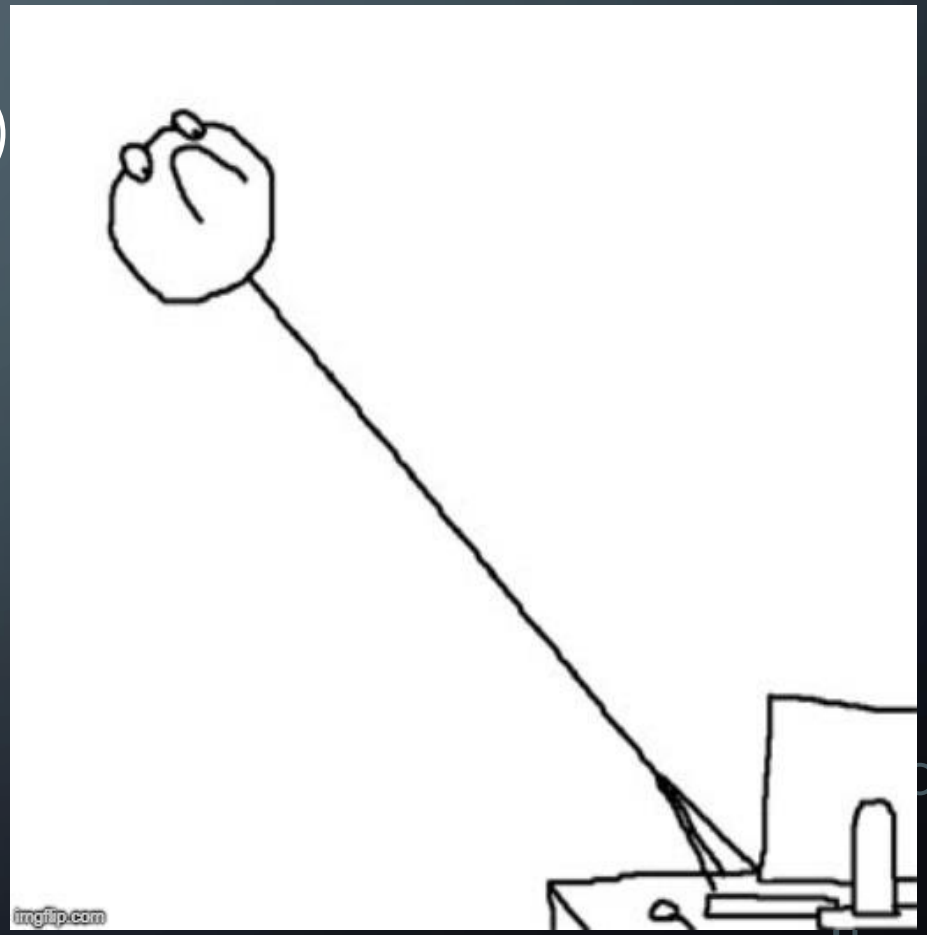


METHOD: MAYBE SPACE?

- PSPACE: Computation in Polynomial Space
- Obviously NP $\subset$ PSPACE
- … well NP $\subseteq$ PSPACE is true!

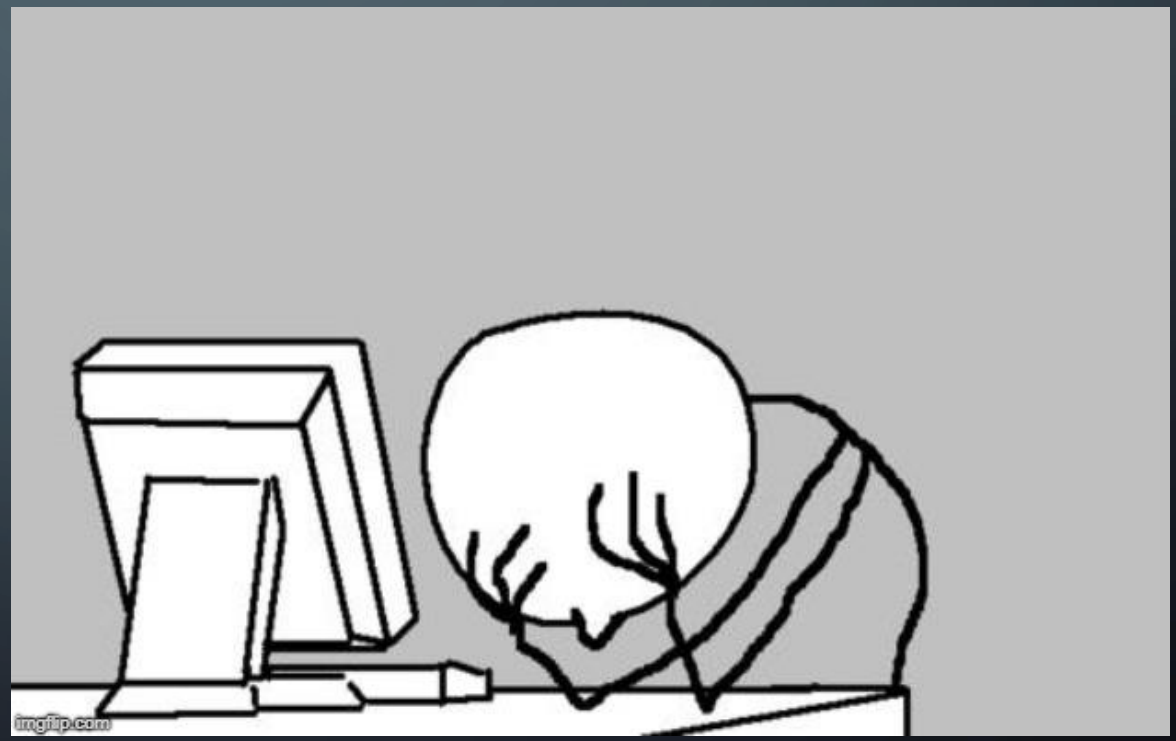
METHOD: WELL…HOW ABOUT RANDOMIZATION?

- BPP (Bounded-Error Probabilistic Polynomial-Time)
  - Accept computation 2/3 if answer is YES
  - Accept computation 1/3 if answer is NO
- $P \stackrel{?}{=} BPP \stackrel{?}{=} NP$
  - BPP is it's own monster



OKAY OKAY… QUANTUM COMPUTING!

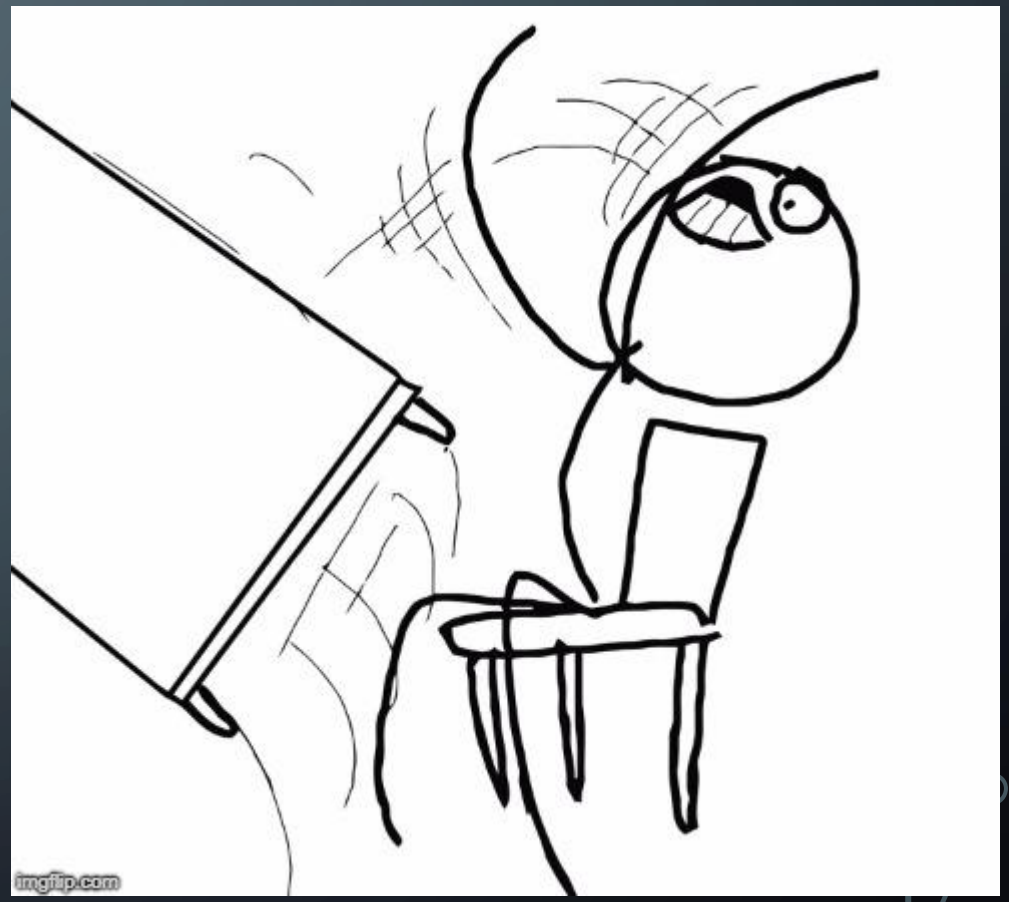
- BQP (Bounded-Error Quantum Polynomial-Time)
  - BPP on Quantum Computer
- Just try everything!
  - Not how QC work!
- Probably BQP ≠ NP



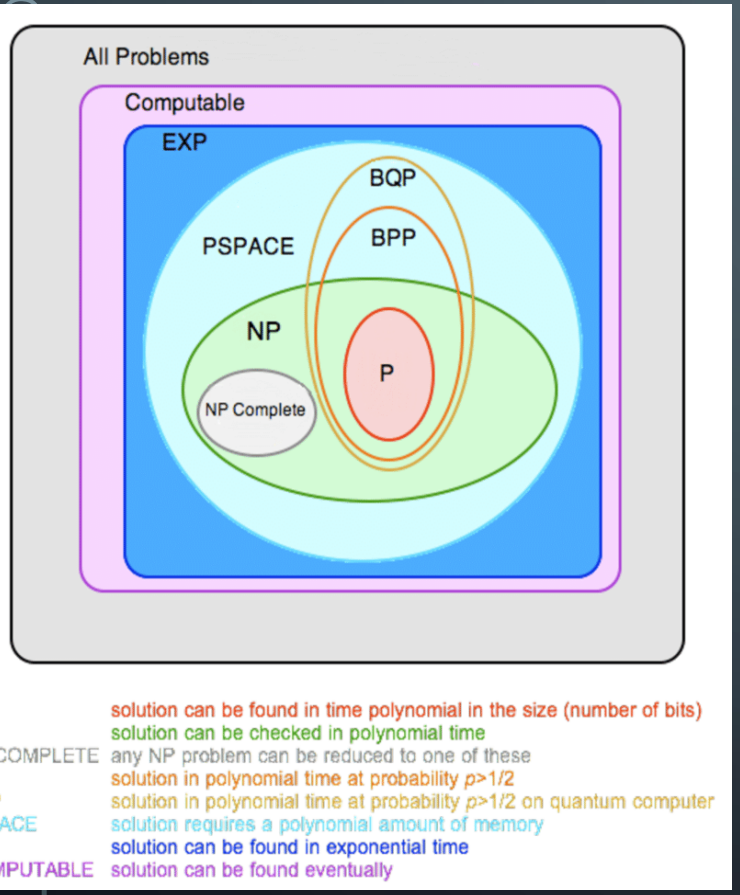
SCREW THIS: LET‘S TRY ORACLES!

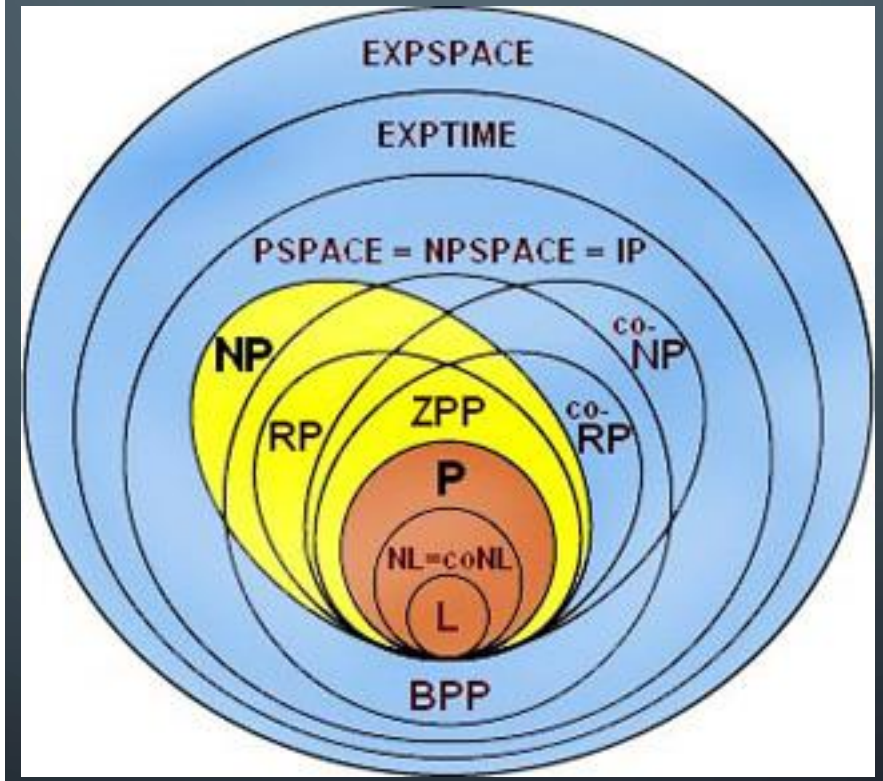
- Let‘s pretend we have an Oracle
  - Knows answer to P or to NP or EXP or …

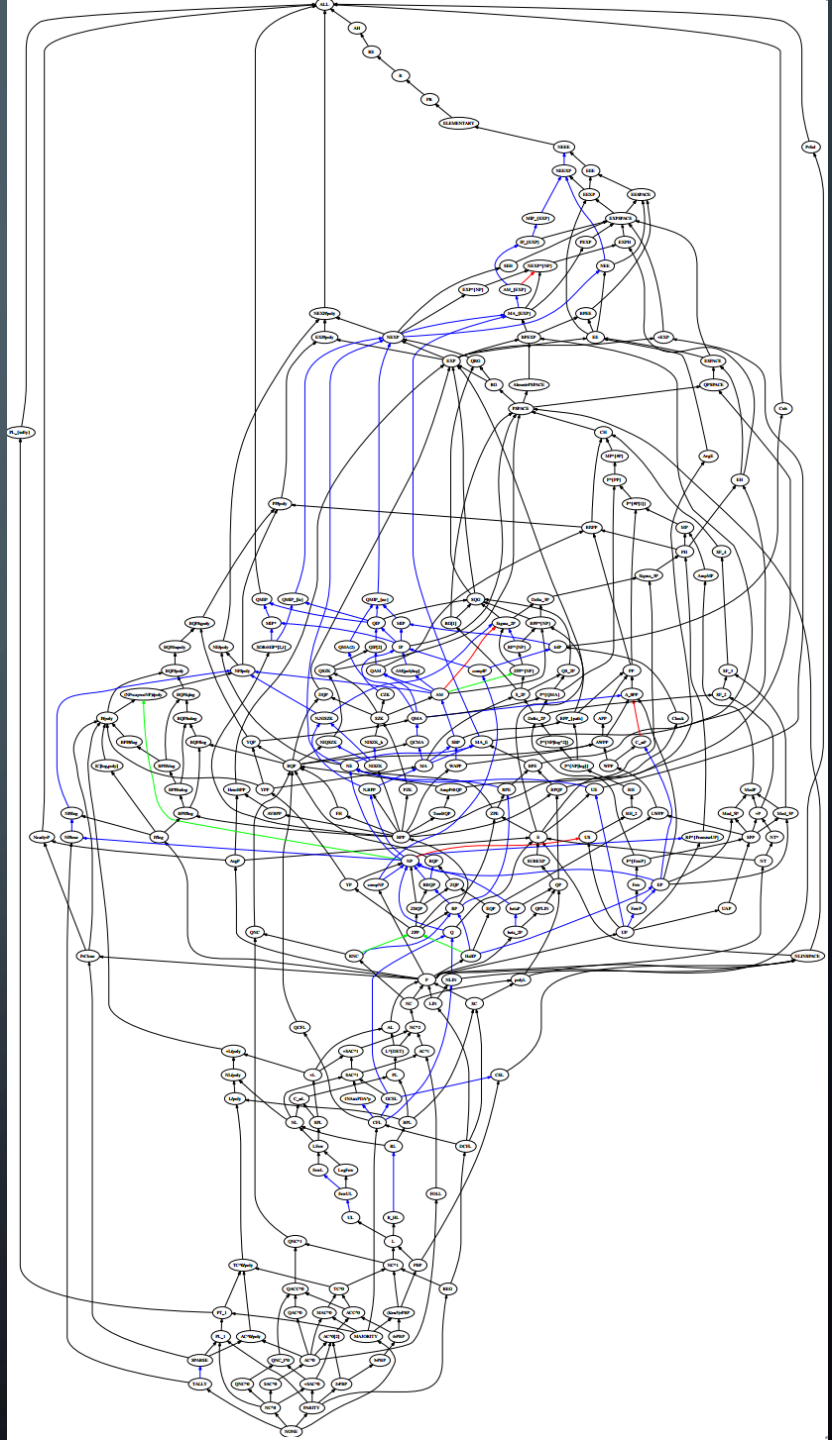
„…the relativized P =? NP question has a positive answer for some oracles and a negative answer for other oracles. We feel that this is further evidence of the difficulty of the P =? NP question.“ Baker, Gill, Solvay



AND THAT WAS JUST A GLIMPSE!







THANKS YOU FOR LISTENING