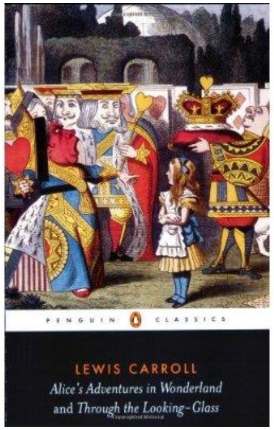
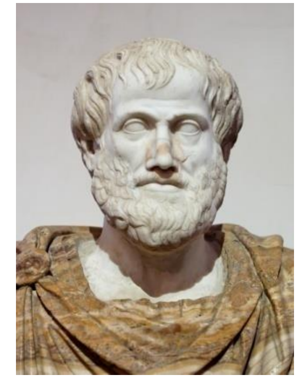


# COMP 1002

# Intro to Logic for Computer Scientists

## Lecture 7


# Admin stuff

- Labs start next Monday/Wednesday
  - Lab 1 posted
- Assignment 1 posted. Due Jan 24
  - We switched to 6 assignments at 5% each
- Midterm: what about Tuesday after the break? Jan 26th?
  - 3 assignments handed in and marked by the drop date, but not the midterm.

# False premises

- An argument can still be valid when some of its premises are false.
  - Remember, false implies anything.
- Bertrand Russell: “If 2+2=5, then I am the pope”
  - Suppose 2+2=5
  - If 2+2=5, then 1=2 (subtract 3 from both sides).
  - So 1=2 (by modus ponens)
  - Me and the pope are two people.
  - Since 1=2, me and the pope are one person.
  - Therefore, I am the pope!

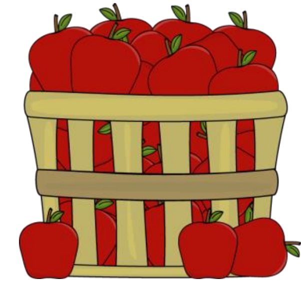
# Natural deduction vs. Truth tables

- In this puzzle, it was faster to solve it using modus ponens (natural deduction method) than writing a truth table.
- But is it always better?
- The answer is...

**Nobody knows!**

- It is a very closely related to the question of how fast can one check if something is a tautology.
  - And that's a million dollar question!

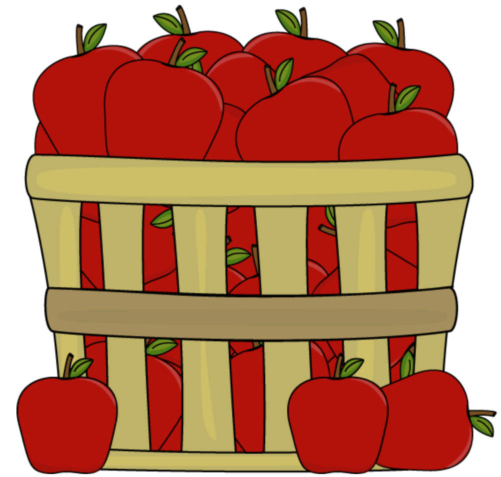
# The million dollar question



- In English, known as "P vs. NP" problem
  - P stands for "polynomial time computable".
  - NP is "polynomial time checkable"
    - non-deterministic polynomial-time computable
  - **Question: is everything efficiently checkable also efficiently computable?**
- In Russian, called "perebor" problem.
  - "perebor" translates as "exhaustive search".
  - Question: is it always possible to avoid looking through nearly all potential solutions to find an answer?
  - **Are there situations when exhaustive search is unavoidable?**

# The million dollar question

- **NP-completeness:** enough to answer for the problem of checking satisfiability (SAT)!

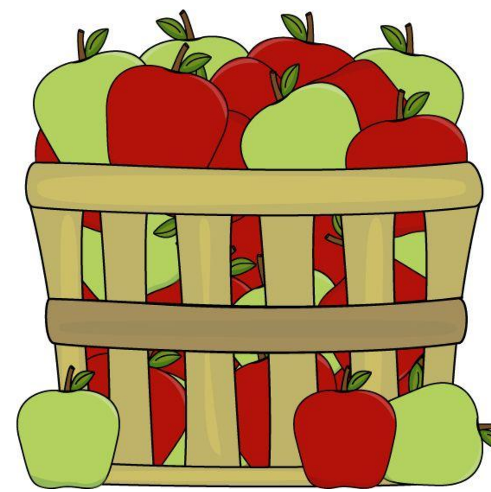


- A formula is like a basket of apples.

  formula is a tautology

  =

  All apples in the basket are good.



- Can you check that all apples are good without looking at every single one?
- Can you do it for every possible basket of apples?
  - Smell test?

# The Millennium Prize Problems

In order to celebrate mathematics in the new millennium, The Clay Mathematics Institute of Cambridge, Massachusetts (CMI) established seven *Prize Problems*. The Prizes were conceived to record some of the most difficult problems with which mathematicians were grappling at the turn of the second millennium; to elevate in the consciousness of the general public the fact that in mathematics, the frontier is still open and abounds in important unsolved problems; to emphasize the importance of working towards a solution of the deepest, most difficult problems; and to recognize achievement in mathematics of historical magnitude.

The prizes were announced at a meeting in Paris, held on May 24, 2000 at the Collège de France. Three lectures were presented: Timothy Gowers spoke on *The Importance of Mathematics*; Michael Atiyah and John Tate spoke on the problems themselves.

The seven Millennium Prize Problems were chosen by the founding Scientific Advisory Board of CMI, which conferred with leading experts worldwide. The focus of the board was on important classic questions that have resisted solution for many years.

Following the decision of the Scientific Advisory Board, the Board of Directors of CMI designated a $7 million prize fund for the solutions to these problems, with $1 million allocated to the solution of each problem.

# Millennium Problems

## Yang–Mills and Mass Gap

Experiment and computer simulations suggest the existence of a "mass gap" in the solution to the quantum versions of the Yang-Mills equations. But no proof of this property is known.

## Riemann Hypothesis

The prime number theorem determines the average distribution of the primes. The Riemann hypothesis tells us about the deviation from the average. Formulated in Riemann's 1859 paper, it asserts that all the 'non-obvious' zeros of the zeta function are complex numbers with real part 1/2.

## P vs NP Problem

If it is easy to check that a solution to a problem is correct, is it also easy to solve the problem? This is the essence of the P vs NP question. Typical of the NP problems is that of the Hamiltonian Path Problem: given N cities to visit, how can one do this without visiting a city twice? If you give me a solution, I can easily check that it is correct. But I cannot so easily find a solution.

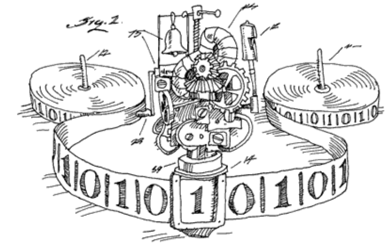
## Navier–Stokes Equation

This is the equation which governs the flow of fluids such as water and air. However, there is no proof for the most basic questions one can ask: do solutions exist, and are they unique? Why ask for a proof? Because a proof gives not only certitude, but also understanding.

## Hodge Conjecture

The answer to this conjecture determines how much of the topology of the solution set of a system of algebraic equations can be defined in terms of further algebraic equations. The Hodge conjecture is known in certain special cases, e.g., when the solution set has dimension less than four. But in

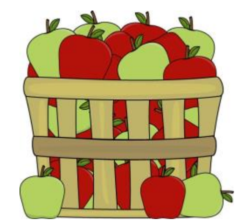
# Automated provers



- How to make an automated prover which checks whether a formula is a tautology?
  - And so can check if an argument is valid, etc.

- Truth tables:
  - easy to program, but proofs are huge.

- Natural deduction:
  - proofs might be smaller than a truth table
    - Are they always? Good question...
  - even if there is a small proof, how can we find one quickly?
    - Nobody knows...



# Resolution proofs


- Middle ground: use the **resolution rule**:
  - Basis for many practical provers (SAT solvers).
  - Used in verification, scheduling, etc...

$$\frac{C \lor x \qquad D \lor \neg x}{\therefore\ C \lor D}$$

$$\frac{y \lor \neg z \lor w \qquad u \lor \neg w}{\therefore\ y \lor \neg z \lor u}$$

$$\frac{y \lor w \lor \neg z \qquad \neg z \lor \neg w}{\therefore\ y \lor \neg z}$$

- Ignore order in an OR and remove duplicates.

# Resolution proofs

- Rather than proving that F is a tautology, prove that $\neg F \equiv FALSE$. That is, a proof of F is a **refutation** of $\neg F$
  - To check that an argument is valid, refute AND of premises AND NOT conclusion.

- Last step of the resolution refutation of $\neg F$:
  - from $x$ and $\neg x$ derive FALSE, for some variable $x$.
  - If you cannot derive anything new, then the formula is satisfiable.

$$(y \vee \neg z) \wedge (\neg y) \wedge (y \vee z)$$

$$(\neg z) \qquad (z)$$

$$FALSE$$

# Puzzle 8

- Suppose that nobody in our class carries more than 10 pens.
- There are 108 students in our class.

- Prove that there are at least 2 students in our class who carry the same number of pens.
  - In fact, there are at least 10 who do.