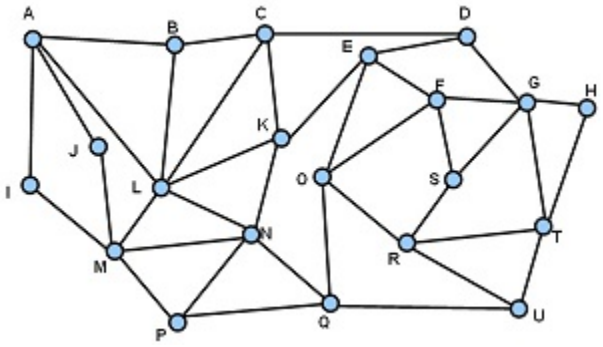
CSCI 270 Lecture 23: The Limits of Knowledge

Independent Set

Given a graph G and an integer k, is there a set of nodes $S \subseteq V$ such that $|S| \geq k$, and there are no edges between two nodes in S?



Vertex Cover

Given a graph G and an integer k, is there a set of nodes $S \subseteq V$ such that $|S| \leq k$ and every edge has at least one endpoint in S?

Set Cover

We are given a set U of n elements, and m subsets $S_1, S_2, ..., S_m \subseteq U$. Given an integer k, is there a collection of $\leq k$ subsets whose union is equal to U?

$S_1 = \{1, 2\}, S_2 = \{2, 3, 5\}, S_3 = \{2, 4\}, S_4 = \{4, 5\}, S_5 = \{3, 6\}, S_6 = \{5, 6\}$

The class NP

Suppose you have an Independent Set example which you have been unable to solve. Albert Einstein walks in, looks at it, and say "Yes! There is an Independent Set of size k, there it is!"

How long would it take you to verify that Albert Einstein's answer is correct?

Suppose Einstein did the same for a Vertex Cover or Set Cover problem. How long would it take you to verify his solution is correct?

A verifier/certifier is like a grader. It does not come up with a solution on its own. It just verifies a given solution is correct.

P is the set of all problems with polynomial-time solutions.

NP is the set of all problems with polynomial-time VERIFIERS.

P=Polynomial Time

NP=Nondeterministic Polynomial Time

Effectively we are saying "If we could guess the solution, we could verify its authenticity in polynomial time".

- What problems have we seen that are in NP?
- Is Sorting in NP?
- Is $P \subseteq NP$?
- Are there problems which are not in NP?
- Is $P \subset NP$?

Alright, let's suppose we want to prove it one way or the other. Here is a possible strategy:

1. Identify the "hardest" problem in NP.
2. Either give a polynomial algorithm for it, or prove no polynomial algorithm is possible.

It's not clear that there is a "hardest" problem in NP, but we should be able to formally define what it **means** to be the hardest problem in NP. What kind of traits do you suppose such a problem would have?

Circuit-SAT

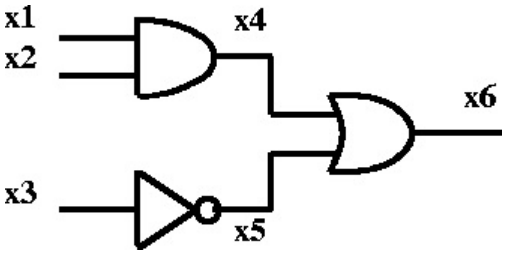
Given a combinational circuit of AND, OR, and NOT gates, is there a way to set the inputs such that the output is 1?

Is Circuit-SAT $\in$ NP?

Figure 1: Futurama, depicting P≠NP.

Figure 2: The Simpsons, depicting P=NP.

Claim: For any problem $x \in \text{NP}$, $x \leq_p$ Circuit-SAT.



- A Turing Machine is a simple mathematical model of a computer. Anything a computer can do, a TM can do (but slowly). TMs are not real things, they are a theoretical concept. Because they are simple, we can formally prove what kinds of things computers can and cannot do.
- A nondeterministic computer is another theoretical concept which does not actually exist. It is effectively an infinitely parallel computer which can try all possible answers simultaneously. Thus, any problem in NP can be solved by a NTM in poly-time, because all it has to do is verify every possible answer in parallel.
- Computers are just circuits. It stands to reason then that we could take a TM and translate it into a circuit which contains the exact same logic.

Effectively: any problem in NP can be reduced to Circuit-SAT in poly-time.

Circuit-SAT is what is called an NP-complete problem:

1. Circuit-SAT $\in$ NP
2. For all $x \in$ NP, $x \leq_P$ Circuit-SAT

Suppose we have another problem Y, and we show:

1. Y $\in$ NP
2. Circuit-SAT $\leq_p$ Y

What have we shown?

Suppose we have another problem Z, and we show:

1. Z $\in$ NP
2. Z $\leq_P$ Circuit-SAT

What have we shown?