M, 11/11/19

Fall’19 CSCE 629

Analysis of Algorithms

Fang Song

Texas A&M U

Lecture 28

- P, NP, NPC

Credit: based on slides by A. smith & K. Wayne

Reflection on reductions

- Basic reduction strategies
  - Reduction by simple equivalence
  - Reduction from special case to general case
  - Reduction by encoding with gadgets

Transitivity. If $X \leq_P Y$ and $Y \leq_P Z$, then $X \leq_P Z$

Proof idea. Compose two reduction algorithms

➔

$$3\text{−SAT} \leq_P \text{INDEPENDENT−SET} \leq_P \text{VERTEX−COVER} \leq_P \text{SET−COVER}$$

Central ideas in complexity

- Poly-time as "feasible"
  - Most natural problems either are easy (e.g., n^3) or no poly-time alg. known
- Reduction : relating hardness ($A \le B \Rightarrow A$ no harder than B)
- Classify problems by "hardness"

Self reducibility

Decision problem. Does there exist a vertex cover of size $\leq k$?
Search problem. Find vertex cover of minimum cardinality.

Self-reducibility. Search problem $\leq_P$ decision version

- Applies to all (NP-complete) problems in this chapter
- Justifies our focus on decision problems
- Ex. Recall HW 1 on 3-SAT

Definition of class P

P. Decision problems for which there is a poly-time algorithm

Problem	Description	Algorithm	YES instance	No instance
Multiple	Is x a multiple of y?	Grade school	51,17	52,17
RELPRIME	Are x and y relatively prime?	Euclid (300 BCE)	34,39	34,51
PRIMES	Is x a prime?	AKS 2002	53	51
EDIT-DISTANCE	Is the edit distance between x and y less than 5?	Dynamic programming	neither either	algorithm quantum

Definition of class NP

NP. Decision problems for which there is a poly-time certifier

Idea of certifier

- Certifier checks a proposed proof π that $s \in X$
- Need not determine whether $s \in X$ on its own

N.B. $|t| = p(|s|)$ for some polynomial $p()$

Def. Algorithm $C(s,t)$ is a certifier for problem X if for every string s, $s \in X$ iff there exists a string t such that $C(s,t) = \text{yes}$

Equivalent def. $\mathbf{NP}$ = nondeterministic polynomial–time

not ~~polynomial~~–time

Certifiers and certificates: Composite

COMPOSITES. Given an integer s, is s composite?

- Certificate: A non-trivial factor t of s.
- Certifier.

```
CompositesCertifier(s,t)
 If (t ≤ 1 or t ≥ s)
     Return false
 Else if (s is a multiple of t)
     Return true
 Else
     Return false
```

- Instance. $s = 437{,}669$
  - Certificate. $t = 541\ or\ 809.\ 437{,}669 = 541 \times 809$

Conclusion. COMPOSITES $\in$ **NP**

Certifiers and certificates: Hamiltonian cycle

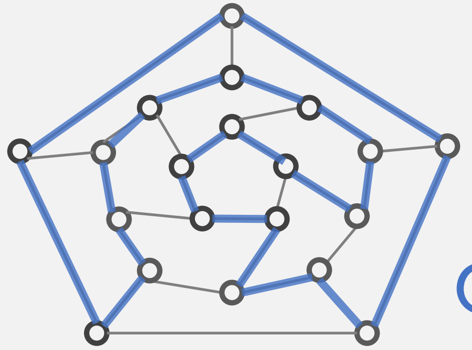
HAM−CYCLE. Given an undirected graph $G = (V, E)$, does there exist a simple cycle that visits every node?

- Certificate: A permutation of n nodes
- Certifier.

HAM-CYCLE-Certifier(G, σ)
  If $(\forall i, j, \sigma_i \neq \sigma_j \,\&(\sigma_i, \sigma_{i+1}) \in E)$
    Return true

Conclusion. HAM−Cycle ∈ **NP**

Instance s



Certificate t

P,NP,EXP

P. Decision problems for which there is a poly-time algorithm

EXP. Decision problems for which $\exists$ an exponential-time algorithm

i.e., runs in time $O(2^{p(|s|)})$ for some polynomial $p()$

NP. Decision problems for which there is a poly-time certifier

- Claim. $\mathbf{P} \subseteq \mathbf{NP} \subseteq \mathbf{EXP}$

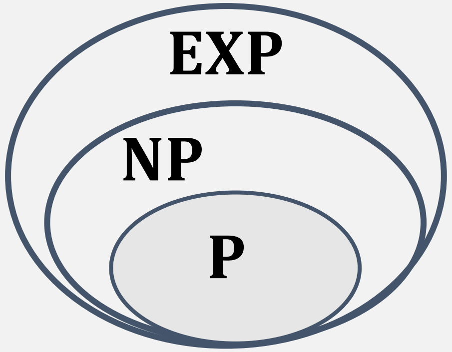
P ⊆ NP. Consider any $X \in \mathrm{P}$,
- $\exists$ poly−time A that solves X
- Certificate: $t = \epsilon$, certifier $C(s,t) = A(s)$

NP ⊆ EXP. Consider any $X \in \mathrm{NP}$,
- $\exists$ poly−time certifier $C(s,t)$
- To decide input s, run $C(s,t)$ on all strings t with $|t| \leq p(|s|)$.
- Return yes, if $C(s,t)$ ever says yes.

Open question: P = NP?

The Millennium prize problems

- $1 million prize



- Consensus opinion on P = NP? Probably no.

Eight Signs A Claimed P≠NP Proof Is Wrong

As of this writing, Vinay Deolalikar still hasn't retracted his P≠NP c

https://www.scottaaronson.com/blog/?p=458

Millennium Problems

Yang–Mills and Mass Gap

Experiment and computer simulations suggest the existence of a "mass gap" in the
no proof of this property is known.

Riemann Hypothesis

The prime number theorem determines the average distribution of the primes. Th
average. Formulated in Riemann's 1859 paper, it asserts that all the 'non-obvious'

P vs NP Problem

If it is easy to check that a solution to a problem is correct, is it also easy to solve th
the NP problems is that of the Hamiltonian Path Problem: given N cities to visit, ho
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. Howeve
solutions exist, and are they unique? Why ask for a proof? Because a proof gives no

Hodge Conjecture

The answer to this conjecture determines how much of the topology of the solutio
further algebraic equations. The Hodge conjecture is known in certain special case
dimension four it is unknown.

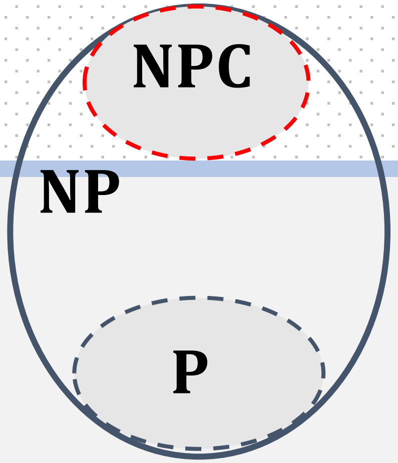
Poincaré Conjecture

In 1904 the French mathematician Henri Poincaré asked if the three dimensional s
manifold. This question, the Poincaré conjecture, was a special case of Thurston's g
three manifold is built from a set of standard pieces, each with one of eight well-ur

Birch and Swinnerton-Dyer Conjecture

Supported by much experimental evidence, this conjecture relates the number of

NP-Completeness



Def. A problem Y is NP-Complete if

1. $Y \in \mathbf{NP}$
2. $\forall X \in \mathbf{NP}, X \leq_{P,Karp} Y$

Theorem. Suppose Y is NP-Complete, then Y is solvable in poly-time iff. $\mathbf{P} = \mathbf{NP}$

Pf.

- ($\Leftarrow$) If $\mathbf{P} = \mathbf{NP}$, then Y can be solved in poly-time since $Y \in \mathbf{NP}$
- ($\Rightarrow$) If Y is solvable in poly-time, consider any $X \in \mathbf{NP}$.

  Since $X \leq_{P,Karp} Y$, X has a poly-time algorithm as well

  I.e., $\mathbf{NP} \subseteq \mathbf{P} \rightarrow \mathbf{P} = \mathbf{NP}$

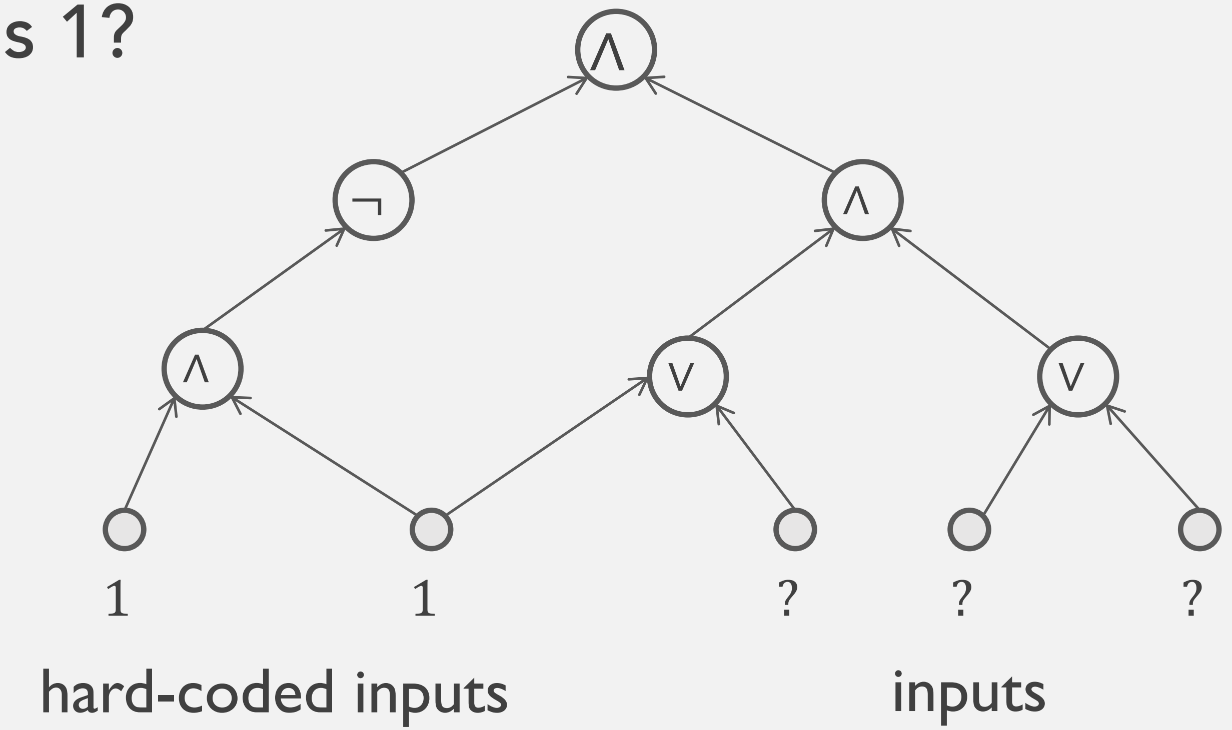
Fundamental question: Are there natural NP-complete problems?

The "first" NP-Complete problem

Theorem. Circuit–SAT is NP-Complete [Cook 1971,Levin 1973]

Input. A combinational circuit built out of AND/OR/NOT gates

Goal. Decide if there is a way to set the circuit inputs so that the output is 1?

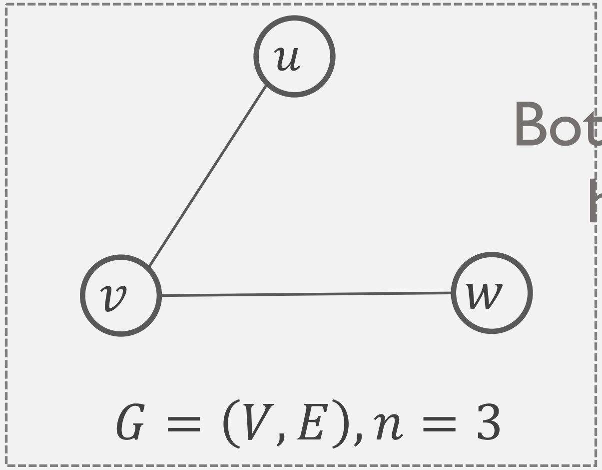


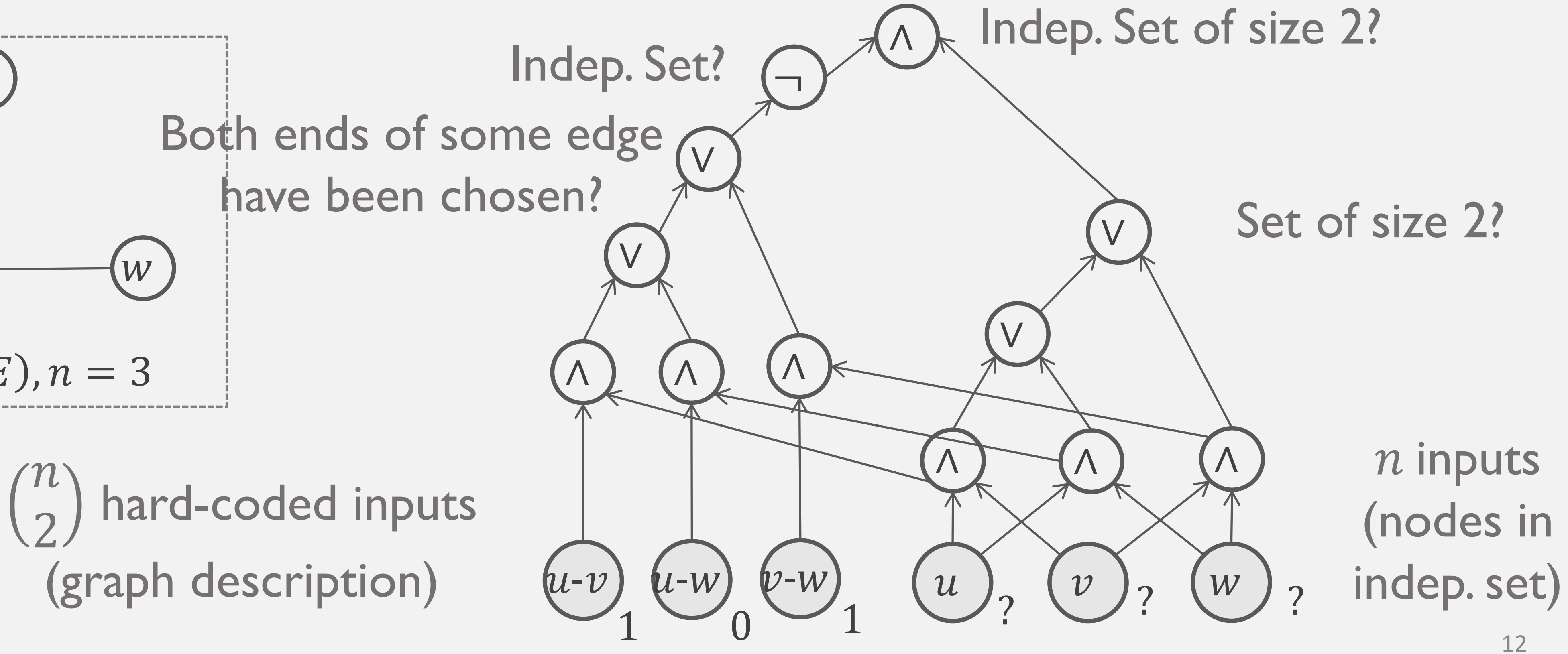
YES! 1 0 1

Example

Given. Graph G

Construction. Circuit K whose inputs can be set so that K outputs true iff. graph G has an independent set of size 2





Establishing NP-Completeness

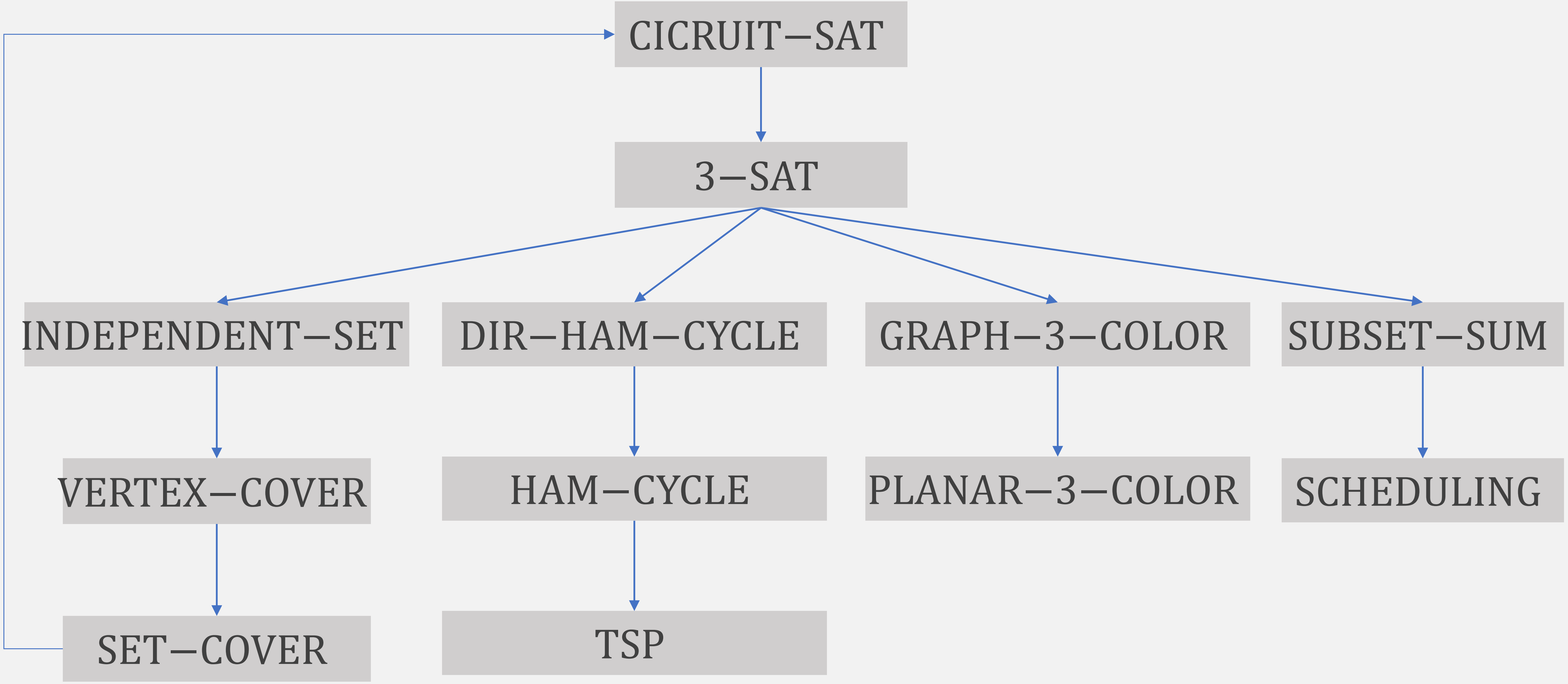
Once we establish first "natural" NP-complete problem, others fall like dominoes …

Recipe to establish NP-Completeness of problem Y

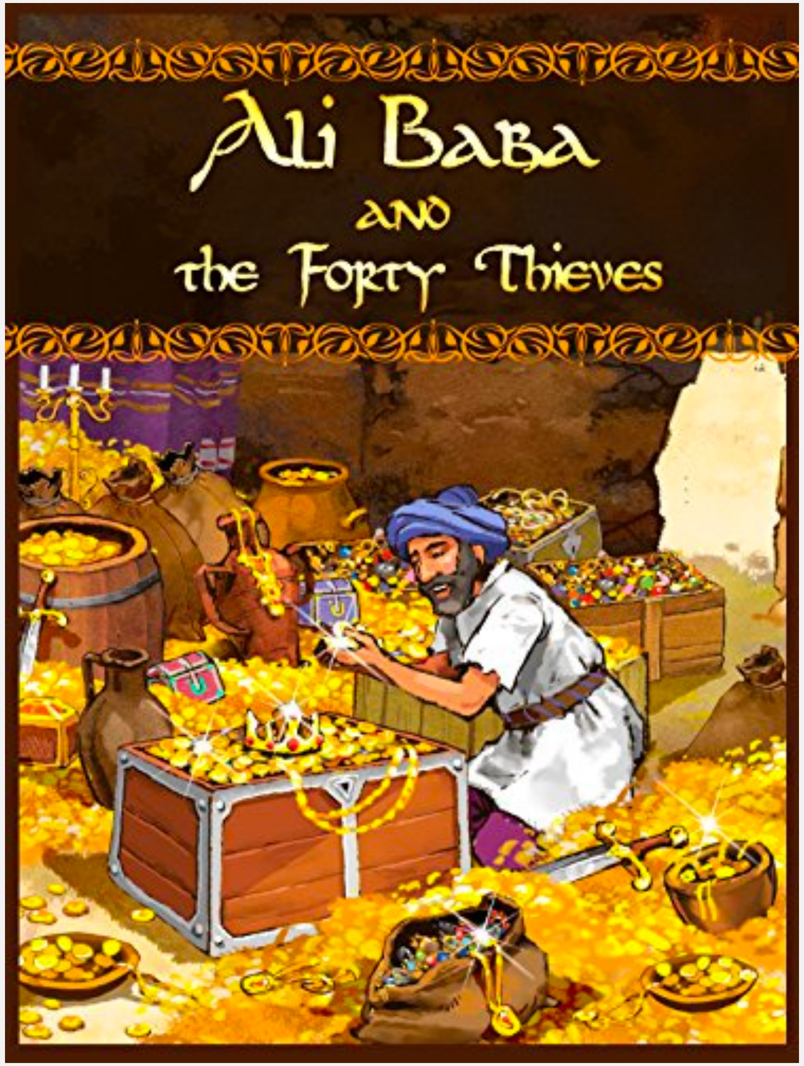
1. Show that $Y \in \mathbf{NP}$
2. Choose an $\mathrm{NP-complete}$ problem X
3. Prove that $X \leq_{P,Karp} Y$

Justification. If X is an NP-complete problem, and Y is a problem in $\mathbf{NP}$ with the property that $X \leq_{P,Karp} Y$ then Y is NP-complete (by transitivity)

NP-Completeness



Alibaba’s knapsack

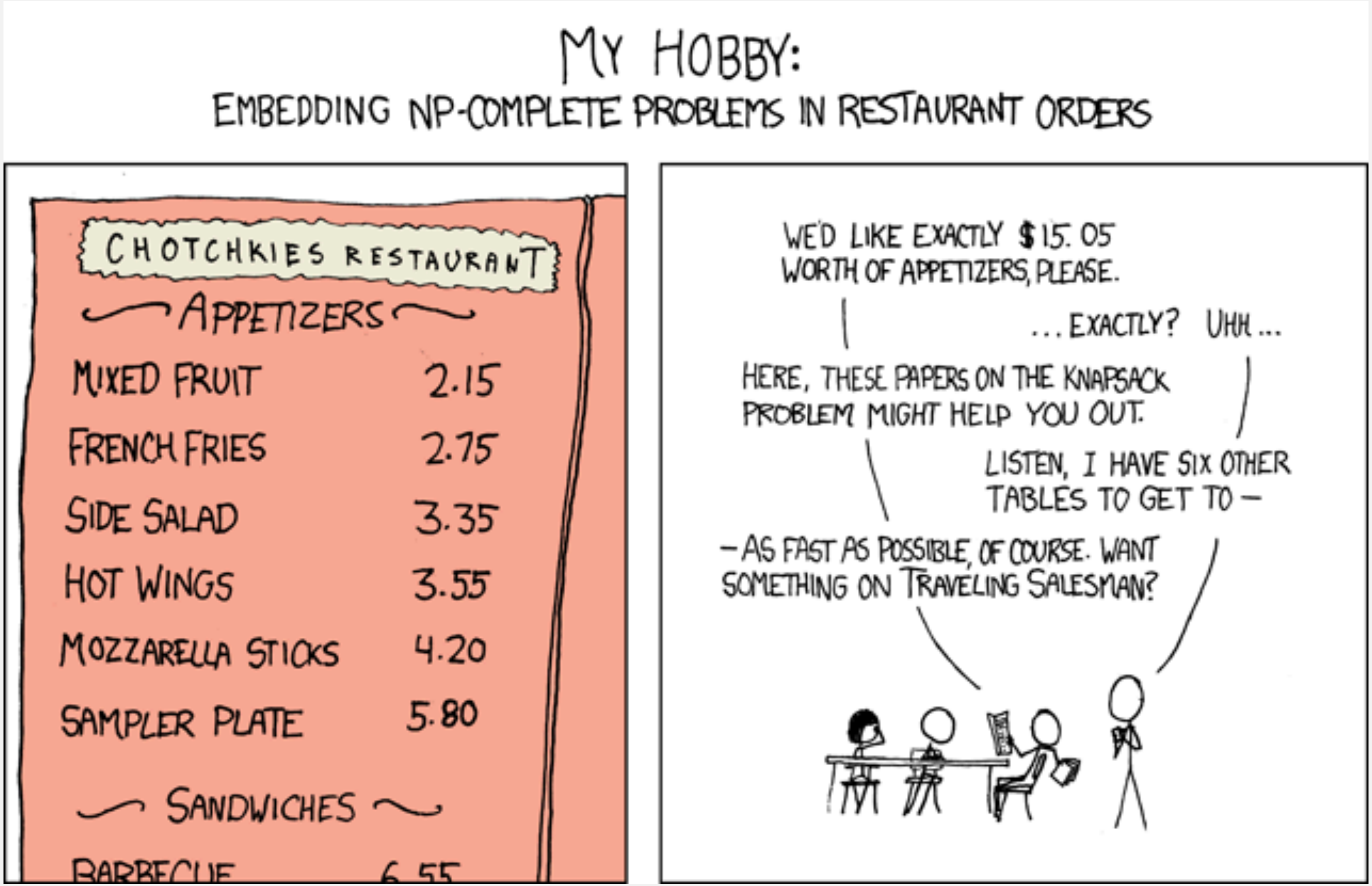


https://images.app.goo.gl/pwGFyw2pp6Xmx6CB8

Modern Version

Alibaba Group

天猫全球狂欢节
2019



https://xkcd.com/287/