8. Intractability II

- P vs. NP
- NP-complete
- co-NP
- NP-hard
Recap

3-SAT poly-time reduces to all of these problems (and many, many more)
8. INTRACTABILITY II

- $P$ vs. $NP$
- $NP$-complete
- $co-NP$
- $NP$-hard
Decision problems

Decision problem.
- Problem $X$ is a set of strings.
- Instance $s$ is one string.
- Algorithm $A$ solves problem $X$: $A(s) = yes$ iff $s \in X$.

Def. Algorithm $A$ runs in polynomial time if for every string $s$, $A(s)$ terminates in at most $p(|s|)$ "steps", where $p(\cdot)$ is some polynomial.

Ex.
- Problem PRIMES = \{ 2, 3, 5, 7, 11, 13, 17, 23, 29, 31, 37, .... \}.
- Instance $s = 592335744548702854681$.
- AKS algorithm PRIMES in $O(|s|^8)$ steps.
**Definition of P**

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

<table>
<thead>
<tr>
<th>Problem</th>
<th>Description</th>
<th>Algorithm</th>
<th>yes</th>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MULTIPLE</strong></td>
<td>Is $x$ a multiple of $y$?</td>
<td>grade-school division</td>
<td>51, 17</td>
<td>51, 16</td>
</tr>
<tr>
<td><strong>REL-PRIME</strong></td>
<td>Are $x$ and $y$ relatively prime?</td>
<td>Euclid (300 BCE)</td>
<td>34, 39</td>
<td>34, 51</td>
</tr>
<tr>
<td><strong>PRIMES</strong></td>
<td>Is $x$ prime?</td>
<td>AKS (2002)</td>
<td>53</td>
<td>51</td>
</tr>
<tr>
<td><strong>EDIT-DISTANCE</strong></td>
<td>Is the edit distance between $x$ and $y$ less than 5?</td>
<td>dynamic programming</td>
<td>neither</td>
<td>acgggt ttttta</td>
</tr>
<tr>
<td><strong>L-SOLVE</strong></td>
<td>Is there a vector $x$ that satisfies $Ax = b$?</td>
<td>Gauss-Edmonds elimination</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>ST-CONN</strong></td>
<td>Is there a path between $s$ and $t$ in a graph $G$?</td>
<td>depth-first search (Theseus)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
NP

Certification algorithm intuition.
• Certifier views things from "managerial" viewpoint.
• Certifier doesn't determine whether $s \in X$ on its own; rather, it checks a proposed proof $t$ that $s \in X$.

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 $C(s, t) = yes$.

Def. NP is the set of problems for which there exists a poly-time certifier.
• $C(s, t)$ is a poly-time algorithm.
• Certificate $t$ is of polynomial size: $|t| \leq p(|s|)$ for some polynomial $p(\cdot)$

Remark. NP stands for nondeterministic polynomial time.
Certifiers and certificates: composite

**COMPOSITES.** Given an integer $s$, is $s$ composite?

**Certificate.** A nontrivial factor $t$ of $s$. Such a certificate exists iff $s$ is composite. Moreover $|t| \leq |s|$.

**Certifier.** Check that $1 < t < s$ and that $s$ is a multiple of $t$.

\[
\begin{array}{|c|c|}
\hline
\text{instance } s & 437669 \\
\text{certificate } t & 541 \text{ or } 809 \\
\hline
\end{array}
\]

\[437,669 = 541 \times 809\]

**Conclusion.** **COMPOSITES $\in$ NP.**
Certifiers and certificates: 3-satisfiability

**3-Sat.** Given a CNF formula \( \Phi \), is there a satisfying assignment?

**Certificate.** An assignment of truth values to the \( n \) boolean variables.

**Certifier.** Check that each clause in \( \Phi \) has at least one true literal.

\[
\text{instance } s \quad \Phi = \left( \overline{x}_1 \lor x_2 \lor x_3 \right) \land \left( x_1 \lor \overline{x}_2 \lor x_3 \right) \land \left( \overline{x}_1 \lor x_2 \lor x_4 \right)
\]

\[
\text{certificate } t \quad x_1 = \text{true}, \; x_2 = \text{true}, \; x_3 = \text{false}, \; x_4 = \text{false}
\]

**Conclusion.** 3-Sat \( \in \mathbf{NP} \).
Certifiers and certificates: Hamilton path

**HAM-PATH.** Given an undirected graph $G = (V, E)$, does there exist a simple path $P$ that visits every node?

**Certificate.** A permutation of the $n$ nodes.

**Certifier.** Check that the permutation contains each node in $V$ exactly once, and that there is an edge between each pair of adjacent nodes.

**Conclusion.** $\text{HAM-PATH} \in \text{NP}$. 
### Definition of NP

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

<table>
<thead>
<tr>
<th>Problem</th>
<th>Description</th>
<th>Algorithm</th>
<th>yes</th>
<th>no</th>
</tr>
</thead>
</table>
| **L-SOLVE** | Is there a vector \( x \) that satisfies \( Ax = b \)? | Gauss-Edmonds elimination | \[
\begin{bmatrix}
0 & 1 & 1 \\
2 & 4 & -2 \\
0 & 3 & 15
\end{bmatrix}, \begin{bmatrix}
4 \\
2 \\
36
\end{bmatrix}
\] | \[
\begin{bmatrix}
1 & 0 & 0 \\
1 & 1 & 1 \\
0 & 1 & 1
\end{bmatrix}, \begin{bmatrix}
1 \\
1 \\
1
\end{bmatrix}
\] |
| **COMPOSITES** | Is \( x \) composite? | AKS (2002)                 | 51           | 53           |
| **FACTOR**  | Does \( x \) have a nontrivial factor less than \( y \)? | ?                          | (56159, 50)  | (55687, 50)  |
| **SAT**     | Is there a truth assignment that satisfies the formula? | ?                          | \( \neg x_1 \lor x_2 \lor x_1 \lor x_2 \lor \neg x_1 \lor x_2 \lor x_1 \lor x_2 \) | |
| **3-COLOR** | Can the nodes of a graph \( G \) be colored with 3 colors? | ?                          | ![3-color-graph](image) | ![3-color-graph](image) |
| **HAM-PATH** | Is there a simple path between \( s \) and \( t \) that visits every node? | ?                          | ![ham-path-graph](image) | ![ham-path-graph](image) |
Definition of NP

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

“NP captures vast domains of computational, scientific, and mathematical endeavors, and seems to roughly delimit what mathematicians and scientists have been aspiring to compute feasibly.” — Christos Papadimitriou

“In an ideal world it would be renamed P vs VP.” — Clyde Kruskal
P, NP, and EXP

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

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

**EXP.** Decision problems for which there is an exponential-time algorithm.

**Claim.** \( P \subseteq NP \).

**Pf.** Consider any problem \( X \in P \).

- By definition, there exists a poly-time algorithm \( A(s) \) that solves \( X \).
- Certificate \( t = \varepsilon \), certifier \( C(s, t) = A(s) \).  

**Claim.** \( NP \subseteq EXP \).

**Pf.** Consider any problem \( X \in NP \).

- By definition, there exists a poly-time certifier \( C(s, t) \) for \( X \).
- To solve input \( s \), run \( C(s, t) \) on all strings \( t \) with \( |t| \leq p(|s|) \).
- Return \( yes \) if \( C(s, t) \) returns \( yes \) for any of these potential certificates.  

**Remark.** Time-hierarchy theorem implies \( P \not\subseteq EXP \).
The main question: P vs. NP

Q. How to solve an instance of 3-SAT with \( n \) variables?
A. Exhaustive search: try all \( 2^n \) truth assignments.

Q. Can we do anything substantially more clever?
Conjecture. No poly-time algorithm for 3-SAT.

"intractable"
The main question: P vs. NP

Does P = NP? [Cook 1971, Edmonds, Levin, Yablonski, Gödel]
Is the decision problem as easy as the certification problem?

If yes. Efficient algorithms for 3-SAT, TSP, 3-COLOR, FACTOR, ...
If no. No efficient algorithms possible for 3-SAT, TSP, 3-COLOR, ...

Consensus opinion. Probably no.
Possible outcomes

P ≠ NP.

“I conjecture that there is no good algorithm for the traveling salesman problem. My reasons are the same as for any mathematical conjecture: (i) It is a legitimate mathematical possibility and (ii) I do not know.”

— Jack Edmonds 1966
Possible outcomes

\[ P \neq NP. \]

“In my view, there is no way to even make intelligent guesses about the answer to any of these questions. If I had to bet now, I would bet that \( P \) is not equal to \( NP \). I estimate the half-life of this problem at 25–50 more years, but I wouldn’t bet on it being solved before 2100.”

— Bob Tarjan

“We seem to be missing even the most basic understanding of the nature of its difficulty…. All approaches tried so far probably (in some cases, provably) have failed. In this sense \( P = NP \) is different from many other major mathematical problems on which a gradual progress was being constantly done (sometimes for centuries) whereupon they yielded, either completely or partially.”

— Alexander Razborov
Possible outcomes

P = NP.

“P = NP. In my opinion this shouldn’t really be a hard problem; it’s just that we came late to this theory, and haven’t yet developed any techniques for proving computations to be hard. Eventually, it will just be a footnote in the books.” — John Conway
Other possible outcomes

**P = NP**, but only \( \Omega(n^{100}) \) algorithm for 3-SAT.

**P \neq NP**, but with \( O(n^{\log^*n}) \) algorithm for 3-SAT.

**P = NP** is independent (of ZFC axiomatic set theory).

“*It will be solved by either 2048 or 4096. I am currently somewhat pessimistic. The outcome will be the truly worst case scenario: namely that someone will prove “P = NP because there are only finitely many obstructions to the opposite hypothesis”; hence there will exists a polynomial time solution to SAT but we will never know its complexity! “*  — Donald Knuth
Millennium prize. $1 million for resolution of $P = NP$ problem.
Looking for a job?

Some writers for the Simpsons and Futurama.

- J. Steward Burns. *M.S. in mathematics (Berkeley '93).*
- David X. Cohen. *M.S. in computer science (Berkeley '92).*
- Al Jean. *B.S. in mathematics. (Harvard '81).*
- Ken Keeler. *Ph.D. in applied mathematics (Harvard '90).*
- Jeff Westbrook. *Ph.D. in computer science (Princeton '89).*
<table>
<thead>
<tr>
<th>char</th>
<th>ASCII</th>
<th>binary</th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
<td>80</td>
<td>1010000</td>
</tr>
<tr>
<td>=</td>
<td>61</td>
<td>0111101</td>
</tr>
<tr>
<td>N</td>
<td>78</td>
<td>1001110</td>
</tr>
<tr>
<td>P</td>
<td>80</td>
<td>1010000</td>
</tr>
<tr>
<td>?</td>
<td>63</td>
<td>0111111</td>
</tr>
</tbody>
</table>
8. **Intractability II**

- $P$ vs. $NP$
- $NP$-complete
- co-$NP$
- $NP$-hard

*Section 8.4*
Polynomial transformation

**Def.** Problem \( X \) polynomial (Cook) reduces to problem \( Y \) if arbitrary instances of problem \( X \) can be solved using:
- Polynomial number of standard computational steps, plus
- Polynomial number of calls to oracle that solves problem \( Y \).

**Def.** Problem \( X \) polynomial (Karp) transforms to problem \( Y \) if given any input \( x \) to \( X \), we can construct an input \( y \) such that \( x \) is a yes instance of \( X \) iff \( y \) is a yes instance of \( Y \).

**Note.** Polynomial transformation is polynomial reduction with just one call to oracle for \( Y \), exactly at the end of the algorithm for \( X \). Almost all previous reductions were of this form.

**Open question.** Are these two concepts the same with respect to \( \textbf{NP} \)?
NP-complete

**NP-complete.** A problem \( Y \in \text{NP} \) with the property that for every problem \( X \in \text{NP} \), \( X \leq_p Y \).

**Theorem.** Suppose \( Y \in \text{NP}\)-complete. Then \( Y \in \text{P} \) iff \( \text{P} = \text{NP} \).

**Pf.** \( \Leftarrow \) If \( \text{P} = \text{NP} \), then \( Y \in \text{P} \) because \( Y \in \text{NP} \).

**Pf.** \( \Rightarrow \) Suppose \( Y \in \text{P} \).

- Consider any problem \( X \in \text{NP} \). Since \( X \leq_p Y \), we have \( X \in \text{P} \).
- This implies \( \text{NP} \subseteq \text{P} \).
- We already know \( \text{P} \subseteq \text{NP} \). Thus \( \text{P} = \text{NP} \). □

**Fundamental question.** Do there exist "natural" \( \text{NP}\)-complete problems?
Circuit satisfiability

CIRCUIT-SAT. Given a combinational circuit built from AND, OR, and NOT gates, is there a way to set the circuit inputs so that the output is 1?

\[
\begin{array}{c}
\text{output} \\
\land \\
\neg \\
\land \\
\land \\
\lor \\
\lor \\
\land \\
1 & 0 & ? & ? & ? \\
\end{array}
\]

yes: 1 0 1
The "first" NP-complete problem

Theorem. CIRCUIT-SAT ∈ NP-complete. [Cook 1971, Levin 1973]

Summary
It is shown that any recognition problem solved by a polynomial time-bound deterministic Turing machine can be "reduced" to the problem of determining whether a given propositional formula is a tautology. Here "reduced" means, roughly speaking, that the first problem can be solved deterministically in polynomial time provided an oracle is available for solving the second. From the notion of reducible, polynomial degrees of difficulty are defined, and it is shown that the problem of determining tautologyhood has the same polynomial degree as the problem of determining whether the first of two given graphs is isomorphic to a subgraph of the second. Other examples are discussed. A method of measuring the complexity of proof procedures for the predicate calculus is introduced and discussed.

1. Tautologies and Polynomial Reducibility.
Let us fix a formalism for the propositional calculus in which formulas are written as strings on T. Since we will require infinitely many proposition symbols (atoms), each such symbol will consist of a member of I and a number in binary notation to distinguish that symbol. Thus a formula of length n can only have about n/logn distinct function and predicate symbols. The logical connectives are ∈ (and), ∧ (or), and ¬ (not).

The set of tautologies (denoted by (tautologies)) is a certain recursive set of strings on this alphabet, and we are interested in the problem of finding a good lower bound on its possible recognition times. We provide no such lower bound here, but theorem 1 will give evidence that (tautologies) is a difficult set to recognize, since many apparently difficult problems can be reduced to determining tautologyhood. By reduced we mean, roughly speaking, that if tautologyhood could be decided instantly (by an "oracle") then these problems could be decided in polynomial time. In order to make this precise, we introduce query machines, which are like Turing machines with oracles in [1].

A query machine is a multitape Turing machine with a distinguished tape called the query tape, and three distinguished states called the query state, yes state, and no state. In computing M is a computation of M in which initially M is in the initial state and and an input string w is on its input tape, and each line M assumes the query state there is a string u on the query tape, and in the next state M assumes in the yes state if uw and the no state if uw. We think of an "oracle", which knows T, placing M in the yes state or no state.

Definition
A set S of strings is P-reducible (P for polynomial) to a set T if strings if for any number of binary query machine M and a polynomial Q(n) such that for each input string w, the computation of M with input w has within Q(n) steps ([w] is the length of w) and ends in an accepting state iff w ∈ S.

It is not hard to see that P-reducibility is a transitive relation. Thus the relation ∈ on
The "first" NP-complete problem

**Theorem.** \( \text{Circuit-Sat} \in \text{NP-complete} \).

**Pf sketch.**

- Clearly, \( \text{Circuit-Sat} \in \text{NP} \).
- Any algorithm that takes a fixed number of bits \( n \) as input and produces a \textit{yes} or \textit{no} answer can be represented by such a circuit.
- Moreover, if algorithm takes poly-time, then circuit is of poly-size.

sketchy part of proof; fixing the number of bits is important, and reflects basic distinction between algorithms and circuits

- Consider any problem \( X \in \text{NP} \). It has a poly-time certifier \( C(s, t) \):
  \( s \in X \) iff there exists a certificate \( t \) of length \( p(|s|) \) such that \( C(s, t) = yes \).
- View \( C(s, t) \) as an algorithm with \( |s| + p(|s|) \) input bits and convert it into a poly-size circuit \( K \).
  - \textit{first} \( |s| \) bits are hard-coded with \( s \)
  - \textit{remaining} \( p(|s|) \) bits represent (unknown) bits of \( t \)
- Circuit \( K \) is satisfiable iff \( C(s, t) = yes \).
**Example**

**Ex.** Construction below creates a circuit $K$ whose inputs can be set so that it outputs 1 iff graph $G$ has an independent set of size 2.

$G = (V, E), n = 3$

<table>
<thead>
<tr>
<th>$u$</th>
<th>$v$</th>
<th>$w$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

Hard-coded inputs

\[
\binom{n}{2} \text{ hard-coded inputs} \quad \binom{n}{2} \text{ (graph description)} \quad n \text{ inputs} \quad (\text{nodes in independent set})
\]
Establishing NP-completeness

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

Recipe. To prove that $Y \in \text{NP}$-complete:
- Step 1. Show that $Y \in \text{NP}$.
- Step 2. Choose an NP-complete problem $X$.
- Step 3. Prove that $X \leq_p Y$.

Theorem. If $X \in \text{NP}$-complete, $Y \in \text{NP}$, and $X \leq_p Y$, then $Y \in \text{NP}$-complete.

Pf. Consider any problem $W \in \text{NP}$. Then, both $W \leq_p X$ and $X \leq_p Y$.
- By transitivity, $W \leq_p Y$.
- Hence $Y \in \text{NP}$-complete. □
3-satisfiability is NP-complete

**Theorem.** \( 3\text{-SAT} \in \text{NP-complete}. \)

**Pf.**
- Suffices to show that \( \text{CIRCUIT-SAT} \leq_p 3\text{-SAT} \) since \( 3\text{-SAT} \in \text{NP}. \)
- Given a combinational circuit \( K \), we construct an instance \( \Phi \) of \( 3\text{-SAT} \) that is satisfiable iff the inputs of \( K \) can be set so that it outputs 1.
3-satisfiability is NP-complete

Construction. Let $K$ be any circuit.

Step 1. Create a 3-SAT variable $x_i$ for each circuit element $i$.

Step 2. Make circuit compute correct values at each node:

- $x_2 = \neg x_3 \implies$ add 2 clauses: $x_2 \lor x_3$,$\quad \neg x_2 \lor \neg x_3$
- $x_1 = x_4 \lor x_5 \implies$ add 3 clauses: $x_1 \lor \neg x_4$,$\quad x_1 \lor \neg x_5$,$\quad \neg x_1 \lor x_4 \lor x_5$
- $x_0 = x_1 \land x_2 \implies$ add 3 clauses: $\neg x_0 \lor x_1$,$\quad \neg x_0 \lor x_2$,$\quad x_0 \lor \neg x_1 \lor \neg x_2$

Step 3. Hard-coded input values and output value.

- $x_5 = 0 \implies$ add 1 clause: $\neg x_5$
- $x_0 = 1 \implies$ add 1 clause: $x_0$
3-satisfiability is NP-complete

Construction. [continued]

Step 4. Turn clauses of length 1 or 2 into clauses of length 3.
   • Create four new variables $z_1$, $z_2$, $z_3$, and $z_4$.
   • Add 8 clauses to force $z_1 = z_2 = false$:

   $$(\overline{z_1} \lor z_3 \lor z_4), \ (\overline{z_1} \lor z_3 \lor \overline{z_4}), \ (\overline{z_1} \lor \overline{z_3} \lor z_4), \ (\overline{z_1} \lor \overline{z_3} \lor \overline{z_4})$$
   $$(\overline{z_2} \lor z_3 \lor z_4), \ (\overline{z_2} \lor z_3 \lor \overline{z_4}), \ (\overline{z_2} \lor \overline{z_3} \lor z_4), \ (\overline{z_2} \lor \overline{z_3} \lor \overline{z_4})$$

   • Replace any clause with a single term $(t_i)$ with $(t_i \lor z_1 \lor z_2)$.
   • Replace any clause with two terms $(t_i \lor t_j)$ with $(t_i \lor t_j \lor z_1)$. 
3-satisfiability is NP-complete

Lemma. \( \Phi \) is satisfiable iff the inputs of \( K \) can be set so that it outputs 1.

\( \Leftarrow \) Suppose there are inputs of \( K \) that make it output 1.
- Can propagate input values to create values at all nodes of \( K \).
- This set of values satisfies \( \Phi \).

\( \Rightarrow \) Suppose \( \Phi \) is satisfiable.
- We claim that the set of values corresponding to the circuit inputs constitutes a way to make circuit \( K \) output 1.
- The 3-SAT clauses were designed to ensure that the values assigned to all node in \( K \) exactly match what the circuit would compute for these nodes. \( \blacksquare \)
Implications of Karp

Circuit-Sat

3-Sat

3-Sat poly-time reduces to Independent-Set

Independent-Set

Directed Ham-Cycle

Graph-3-Color

Subset-Sum

Vertex-Cover

Ham-Cycle

Planar-3-Color

Scheduling

Circuit-Sat poly-time reduces to all of these problems (and many, many more)
Implications of Cook-Levin

All of these problems (and many, many more) poly-time reduce to CIRCUIT-SAT.
Implications of Karp + Cook-Levin

All of these problems are NP-complete; they are manifestations of the same really hard problem.
Some NP-complete problems

Basic genres of NP-complete problems and paradigmatic examples.
- Packing + covering problems: SET-COVER, VERTEX-COVER, INDEPENDENT-SET.
- Constraint satisfaction problems: CIRCUIT-SAT, SAT, 3-SAT.
- Sequencing problems: HAM-CYCLE, TSP.
- Partitioning problems: 3D-MATCHING, 3-COLOR.
- Numerical problems: SUBSET-SUM, PARTITION.

Practice. Most NP problems are known to be either in P or NP-complete.

Notable exceptions. FACTOR, GRAPH-ISOMORPHISM, NASH-EQUILIBRIUM.

Theory. [Ladner 1975] Unless P = NP, there exist problems in NP that are neither in P nor NP-complete.
More hard computational problems

**Garey and Johnson.** Computers and Intractability.

- Appendix includes over 300 NP-complete problems.
- Most cited reference in computer science literature.

---

**Most Cited Computer Science Citations**

This list is generated from documents in the CiteSeerX database as of January 17, 2013. This list is automatically generated and may contain errors. The list is generated in batch mode and citation counts may differ from those currently in the CiteSeerX database, since the database is continuously updated.


1. M R Garey, D S Johnson
   8655
2. T Cormen, C E Leiserson, R Rivest
   *Introduction to Algorithms* 1990
   7210
3. V N Vapnik
   *The nature of statistical learning theory* 1998
   6580
4. A P Dempster, N M Laird, D B Rubin
   *Maximum likelihood from incomplete data via the EM algorithm.* Journal of the Royal Statistical Society, 1977
   6082
5. T Cover, J Thomas
   *Elements of Information Theory* 1991
   6075
6. D E Goldberg
   5998
7. J Pearl
   *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference* 1988
   5582
8. E Gamma, R Helm, R Johnson, J Vlissides
   *Design Patterns: Elements of Reusable Object-Oriented Software* 1995
   4614
9. C E Shannon
   *A mathematical theory of communication* Bell Syst. Tech. J., 1948
   4118
10. J R Quinlan
    *C4.5: Programs for Machine Learning* 1993
    4018
More hard computational problems

**Aerospace engineering.** Optimal mesh partitioning for finite elements.

**Biology.** Phylogeny reconstruction.

**Chemical engineering.** Heat exchanger network synthesis.

**Chemistry.** Protein folding.

**Civil engineering.** Equilibrium of urban traffic flow.

**Economics.** Computation of arbitrage in financial markets with friction.

**Electrical engineering.** VLSI layout.

**Environmental engineering.** Optimal placement of contaminant sensors.

**Financial engineering.** Minimum risk portfolio of given return.

**Game theory.** Nash equilibrium that maximizes social welfare.

**Mathematics.** Given integer $a_1, \ldots, a_n$, compute

$$\int_0^{2\pi} \cos(a_1 \theta) \times \cos(a_2 \theta) \times \cdots \times \cos(a_n \theta) \, d\theta$$

**Mechanical engineering.** Structure of turbulence in sheared flows.

**Medical engineering.** Reconstructing 3d shape from biplane angiocardiogram.

**Operations research.** Traveling salesperson problem.

**Physics.** Partition function of 3d Ising model.

**Politics.** Shapley-Shubik voting power.

**Recreation.** Versions of Sudoku, Checkers, Minesweeper, Tetris.

**Statistics.** Optimal experimental design.
Extent and impact of NP-completeness

Extent of NP-completeness. [Papadimitriou 1995]
- Prime intellectual export of CS to other disciplines.
- 6,000 citations per year (more than "compiler", "OS", "database").
- Broad applicability and classification power.

NP-completeness can guide scientific inquiry.
- 1926: Ising introduces simple model for phase transitions.
- 1944: Onsager finds closed-form solution to $2\text{D-ISING}$ in tour de force.
- 19xx: Feynman and other top minds seek solution to $3\text{D-ISING}$.
- 2000: Istrail proves $3\text{D-ISING} \in \text{NP-complete}$.

search for closed formula appears doomed

a holy grail of statistical mechanics
P vs. NP revisited

Overwhelming consensus (still). \( P \neq NP \).

Why we believe \( P \neq NP \).

“We admire Wiles' proof of Fermat's last theorem, the scientific theories of Newton, Einstein, Darwin, Watson and Crick, the design of the Golden Gate bridge and the Pyramids, precisely because they seem to require a leap which cannot be made by everyone, let alone a by simple mechanical device.” — Avi Wigderson
You NP-complete me
8. INTRACTABILITY II

- P vs. NP
- NP-complete
- co-NP
- NP-hard

Section 8.9
Asymmetry of NP

Asymmetry of NP. We only need to have short proofs of \textit{yes} instances.

\textbf{Ex 1. SAT vs. Tautology.}
\begin{itemize}
  \item Can prove a CNF formula is satisfiable by specifying an assignment.
  \item How could we prove that a formula is not satisfiable?
\end{itemize}

\textbf{Ex 2. Ham-Cycle vs. No-Ham-Cycle.}
\begin{itemize}
  \item Can prove a graph is Hamiltonian by specifying a permutation.
  \item How could we prove that a graph is not Hamiltonian?
\end{itemize}

\textbf{Q.} How to classify Tautology and No-Hamilton-Cycle?
\begin{itemize}
  \item \textsc{Sat} \(\in\) \textbf{NP}-complete and \textsc{Sat} \(\equiv_p\) Tautology.
  \item \textsc{Ham-Cycle} \(\in\) \textbf{NP}-complete and \textsc{Ham-Cycle} \(\equiv_p\) No-Ham-Cycle.
  \item But neither Tautology nor No-Ham-Cycle are known to be in NP.
\end{itemize}
NP and co-NP

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

**Ex.** SAT, HAMILTON-CYCLE, and COMPOSITE.

**Def.** Given a decision problem $X$, its complement $\overline{X}$ is the same problem with the *yes* and *no* answers reverse.

**Ex.** $X = \{0, 1, 4, 6, 8, 9, 10, 12, 14, 15, \ldots \}$

$\overline{X} = \{2, 3, 5, 7, 11, 13, 17, 23, 29, \ldots \}$

**co-NP.** Complements of decision problems in **NP**.

**Ex.** TAUTOLOGY, NO-HAMILTON-CYCLE, and PRIMES.
NP = co-NP?

Fundamental open question. Does $\text{NP} = \text{co-NP}$?

- Do *yes* instances have succinct certificates iff *no* instances do?
- Consensus opinion: no.

Theorem. If $\text{NP} \neq \text{co-NP}$, then $\text{P} \neq \text{NP}$.

Pf idea.

- $\text{P}$ is closed under complementation.
- If $\text{P} = \text{NP}$, then $\text{NP}$ is closed under complementation.
- In other words, $\text{NP} = \text{co-NP}$.
- This is the contrapositive of the theorem.
Good characterizations

**Good characterization.** [Edmonds 1965] \( \text{NP} \cap \text{co-NP}. \)

- If problem \( X \) is in both \( \text{NP} \) and \( \text{co-NP} \), then:
  - for *yes* instance, there is a succinct certificate
  - for *no* instance, there is a succinct disqualifier
- Provides conceptual leverage for reasoning about a problem.

**Ex.** Given a bipartite graph, is there a perfect matching.
- If yes, can exhibit a perfect matching.
- If no, can exhibit a set of nodes \( S \) such that \( |N(S)| < |S| \).
We seek a good characterization of the minimum number of independent sets into which the columns of a matrix of $M_F$ can be partitioned. As the criterion of “good” for the characterization we apply the “principle of the absolute supervisor.” The good characterization will describe certain information about the matrix which the supervisor can require his assistant to search out along with a minimum partition and which the supervisor can then use with ease to verify with mathematical certainty that the partition is indeed minimum. Having a good characterization does not mean necessarily that there is a good algorithm. The assistant might have to kill himself with work to find the information and the partition.
Good characterizations

Observation. \( P \subseteq NP \cap co-NP \).
- Proof of max-flow min-cut theorem led to stronger result that max-flow and min-cut are in \( P \).
- Sometimes finding a good characterization seems easier than finding an efficient algorithm.

Fundamental open question. Does \( P = NP \cap co-NP \)?
- Mixed opinions.
- Many examples where problem found to have a nontrivial good characterization, but only years later discovered to be in \( P \).
Linear programming is in $\text{NP} \cap \text{co-NP}$

**Linear programming.** Given $A \in \mathbb{R}^{m \times n}$, $b \in \mathbb{R}^m$, $c \in \mathbb{R}^n$, and $\alpha \in \mathbb{R}$, does there exist $x \in \mathbb{R}^n$ such that $Ax \leq b$, $x \geq 0$ and $c^T x \geq \alpha$?

**Theorem.** [Gale-Kuhn-Tucker 1948] $\text{LINEAR-PROGRAMMING } \in \text{ NP } \cap \text{ co-NP}$. 

**Pf sketch.** If (P) and (D) are nonempty, then $\max = \min$.

\[\begin{align*}
\text{(P)} \quad & \max c^T x \\
& \text{s. t. } Ax \leq b \\
& \quad x \geq 0 \\
\text{(D)} \quad & \min y^T b \\
& \text{s. t. } A^T y \geq c \\
& \quad y \geq 0
\end{align*}\]
Linear programming is in $\text{NP} \cap \text{co-NP}$

**Linear programming.** Given $A \in \mathbb{R}^{m \times n}$, $b \in \mathbb{R}^m$, $c \in \mathbb{R}^n$, and $\alpha \in \mathbb{R}$, does there exist $x \in \mathbb{R}^n$ such that $Ax \leq b$, $x \geq 0$ and $c^T x \geq \alpha$?

**Theorem.** [Khachiyan 1979] $\text{LINEAR-PROGRAMMING} \in \text{P}$. 
Primality testing is in $\text{NP} \cap \text{co-NP}$

**Theorem.** [Pratt 1975] $\text{PRIMES} \in \text{NP} \cap \text{co-NP}$. 

---

**EVERY PRIME HAS A SUCCINCT CERTIFICATE**

**VAUGHAN R. PRATT**

**Abstract.** To prove that a number $n$ is composite, it suffices to exhibit the working for the multiplication of a pair of factors. This working, represented as a string, is of length bounded by a polynomial in $\log_2 n$. We show that the same property holds for the primes. It is noteworthy that almost no other set is known to have the property that short proofs for membership or nonmembership exist for all candidates without being known to have the property that such proofs are easy to come by. It remains an open problem whether a prime $n$ can be recognized in only $\log_2 n$ operations of a Turing machine for any fixed $x$.

The proof system used for certifying primes is as follows.

**Axiom.** $(x, y, 1)$.

**Inference Rules.**

- $R_1: (p, x, a), q \vdash (p, x, qa)$ provided $x^{(n-1)/q} \not\equiv 1 \pmod{p}$ and $q|(p - 1)$.
- $R_2: (p, x, p - 1) \vdash p$ provided $x^{p-1} \equiv 1 \pmod{p}$.

**Theorem 1.** $p$ is a theorem $\equiv p$ is a prime.

**Theorem 2.** $p$ is a theorem $\Rightarrow p$ has a proof of $[4\log_2 p]$ lines.
Primality testing is in \( \text{NP} \cap \text{co-NP} \)

**Theorem.** [Pratt 1975] \( \text{PRIMES} \in \text{NP} \cap \text{co-NP}. \)

**Pf sketch.** An odd integer \( s \) is prime iff there exists an integer \( 1 < t < s \) s.t.

\[
\begin{align*}
t^{s-1} &\equiv 1 \pmod{s} \\
t^{(s-1)/p} &\not\equiv 1 \pmod{s}
\end{align*}
\]

for all prime divisors \( p \) of \( s-1 \)

**Certifier** \((s)\)

**Check** \( s - 1 = 2 \times 2 \times 3 \times 36473 \).

**Check** \( 17^{s-1} \equiv 1 \pmod{s} \).

**Check** \( 17^{(s-1)/2} \equiv 437676 \pmod{s} \).

**Check** \( 17^{(s-1)/3} \equiv 329415 \pmod{s} \).

**Check** \( 17^{(s-1)/36473} \equiv 305452 \pmod{s} \).

prime factorization of \( s-1 \)
also need a recursive certificate
to assert that 3 and 36,473 are prime

use repeated squaring
Primality testing is in $P$}

**Theorem.** [Agrawal-Kayal-Saxena 2004] $\text{PRIMES} \in P$.

---

Annals of Mathematics, **160** (2004), 781–793

**PRIMES is in $P$**

By **Manindra Agrawal**, **Neeraj Kayal**, and **Nitin Saxena**

**Abstract**

We present an unconditional deterministic polynomial-time algorithm that determines whether an input number is prime or composite.
Factoring is in $\text{NP} \cap \text{co-NP}$

**FACTORIZER.** Given an integer $x$, find its prime factorization.

**FACTOR.** Given two integers $x$ and $y$, does $x$ have a nontrivial factor $< y$?

**Theorem.** $\text{FACTOR} \equiv_p \text{FACTORIZER}$.

**Pf.**

- $\leq_p$ trivial.
- $\geq_p$ binary search to find a factor; divide out the factor and repeat. □

**Theorem.** $\text{FACTOR} \in \text{NP} \cap \text{co-NP}$.

**Pf.**

- Certificate: a factor $p$ of $x$ that is less than $y$.
- Disqualifier: the prime factorization of $x$ (where each prime factor is less than $y$), along with a Pratt certificate that each factor is prime. □
Is factoring in \( P \) ?

**Fundamental question.** Is \( \text{FACTOR} \in P \).

**Challenge.** Factor this number.

\[
74037563479561712828046796097429573142593188889231289 \\
08493623263897276503402826627689199641962511784399589 \\
43305021275853701189680982867331732731089309005525051 \\
16877063299072396380786710086096962537934650563796359
\]

RSA-704
($30,000 prize if you can factor)
Exploiting intractability

Modern cryptography.
- Ex. Send your credit card to Amazon.
- Ex. Digitally sign an e-document.
- Enables freedom of privacy, speech, press, political association.

RSA. Based on dichotomy between complexity of two problems.
- To use: generate two random $n$-bit primes and multiply.
- To break: suffices to factor a $2n$-bit integer.

\[
\begin{align*}
& P \neq Q, \text{ PRIME} \\
& N = PQ \\
& ED = 1 \mod (P-1)(Q-1) \\
& C = M^E \mod N \\
& M = C^D \mod N
\end{align*}
\]

The RSA algorithm is the most widely used method of implementing public key cryptography and has been deployed in more than one billion applications worldwide.

RSA algorithm

RSA sold for $2.1$ billion

or design a t-shirt
Factoring on a quantum computer

**Theorem.** [Shor 1994] Can factor an $n$-bit integer in $O(n^3)$ steps on a "quantum computer."

2001. Factored $15 = 3 \times 5$ (with high probability) on a quantum computer.

2012. Factored $21 = 3 \times 7$.

**Fundamental question.** Does $P = BQP$?
8. **INTRACTABILITY II**

- $P$ vs. $NP$
- $NP$-complete
- $co-NP$
- $NP$-hard
A note on terminology

A TERMINOLOGICAL PROPOSAL

D. F. Knuth

While preparing a book on combinatorial algorithms, I felt a strong need for a new technical term, a word which is essentially a one-sided version of polynomial complete. A great many problems of practical interest have the property that they are at least as difficult to solve in polynomial time as those of the Cook-Karp class NP. I needed an adjective to convey such a degree of difficulty, both formally and informally; and since the range of practical applications is so broad, I felt it would be best to establish such a term as soon as possible.

The goal is to find an adjective $x$ that sounds good in sentences like this:

The covering problem is $x$.
It is $x$ to decide whether a given graph has a Hamiltonian circuit.
It is unknown whether or not primality testing is an $x$ problem.

Note. The term $x$ does not necessarily imply that a problem is in \textbf{NP}, just that every problem in \textbf{NP} poly-time reduces to $x$. 

61
A note on terminology

Knuth's original suggestions.

- Hard.
- Tough.  
- Herculean.
- Formidable.
- Arduous.

assign a real number between 0 and 1 to each choice

so common that it is unclear whether it is being used in a technical sense
A note on terminology

Some English word write-ins.

- Impractical.
- Bad.
- Heavy.
- Tricky.
- Intricate.
- Prodigious.
- Difficult.
- Intractable.
- Costly.
- Obdurate.
- Obstinate.
- Exorbitant.
- Interminable.
A note on terminology

**Hard-boiled.** [Ken Steiglitz] In honor of Cook.


**Sisyphean.** [Bob Floyd] Problem of Sisyphus was time-consuming.

**Ulyssean.** [Don Knuth] Ulysses was known for his persistence.

“creative research workers are as full of ideas for new terminology as they are empty of enthusiasm for adopting it.”

— Donald Knuth
A note on terminology: acronyms

**PET.** [Shen Lin] Probably exponential time.
- If $P \neq NP$, provably exponential time.
- If $P = NP$, previously exponential time.

**GNP.** [Al Meyer] Greater than or equal to $NP$ in difficulty.
- And costing more than the GNP to solve.
A note on terminology: made-up words

**Exparent.** [Mike Paterson] Exponential + apparent.

**Perarduous.** [Mike Paterson] Through (in space or time) + completely.

**Supersat.** [Al Meyer] Greater than or equal to satisfiability.

**Polychronious.** [Ed Reingold] Enduringly long; chronic.
A note on terminology: consensus

**NP-complete.** A problem in **NP** such that every problem in **NP** poly-time reduces to it.

**NP-hard.** [Bell Labs, Steve Cook, Ron Rivest, Sartaj Sahni]
A problem such that every problem in **NP** polynomial-time reduces to it.

One final criticism (which applies to all the terms suggested) was stated nicely by Vaughan Pratt: "If the Martians know that $P = NP$ for Turing Machines and they kidnap me, I would lose face calling these problems 'formidable'." Yes; if $P = NP$, there's no need for any term at all. But I'm willing to risk such an embarrassment, and in fact I'm willing to give a prize of one live turkey to the first person who proves that $P = NP$. 