7.8 Intractability

Properties of Algorithms

Q. Which algorithms are useful in practice?

A working definition. [von Neumann 1953, Gödel 1956, Cobham 1964, Edmonds 1965, Rabin 1966]
- Model of computation = deterministic Turing machine.
- Measure running time as a function of input size N.
- Efficient = polynomial time for all inputs.

$a N^b$

> Ex 1. Sorting N elements takes N^2 steps using insertion sort.
> Ex 2. Finding best TSP tour on N elements takes N! steps using exhaustive search.

Theory. Definition is broad and robust.
Practice. Poly-time algorithms scale to huge problems.

constants a and b tend to be small

Exponential Growth

Exponential growth dwarfs technological change.
- Suppose you have a giant parallel computing device…
- With as many processors as electrons in the universe…
- And each processor has power of today's supercomputers…
- And each processor works for the life of the universe…

Quantity	Value
electrons in universe †	10^{79}
supercomputer instructions per second	10^{13}
age of universe in seconds †	10^{17}

† Estimated

- Will not help solve 1,000 city TSP problem via brute force.

$1000! \gg 10^{1000} \gg 10^{79} \times 10^{13} \times 10^{17}$

Properties of Problems

Q. Which problems can we solve in practice?
A. Those with poly-time algorithms.

Q. Which problems have poly-time algorithms?
A. No easy answers. Focus of today's lecture.

Three Fundamental Problems

LSOLVE. Given a system of linear equations, find a solution.

$$\begin{array}{rrrcr} 0x_0 & + 1x_1 & + 1x_2 & = & 4 \\ 2x_0 & + 4x_1 & - 2x_2 & = & 2 \\ 0x_0 & + 3x_1 & + 15x_2 & = & 36 \end{array} \qquad \begin{array}{rcr} x_0 & = & -1 \\ x_1 & = & 2 \\ x_2 & = & 2 \end{array}$$

LP. Given a system of linear inequalities, find a solution.

$$\begin{array}{rrrcr} 48x_0 & + 16x_1 & + 119x_2 & \le & 88 \\ 5x_0 & + 4x_1 & + 35x_2 & \ge & 13 \\ 15x_0 & + 4x_1 & + 20x_2 & \ge & 23 \\ x_0 & , \ x_1 & , \ x_2 & \ge & 0 \end{array} \qquad \begin{array}{rcr} x_0 & = & 1 \\ x_1 & = & 1 \\ x_2 & = & \tfrac{1}{5} \end{array}$$

ILP. Given a system of linear inequalities, find a binary solution.

$$\begin{array}{rrrcr} & x_1 & + x_2 & \ge & 1 \\ x_0 & & + x_2 & \ge & 1 \\ x_0 & + x_1 & + x_2 & \le & 2 \end{array} \qquad \begin{array}{rcr} x_0 & = & 0 \\ x_1 & = & 1 \\ x_2 & = & 1 \end{array}$$

Three Fundamental Problems

LSOLVE. Given a system of linear equations, find a solution.
LP. Given a system of linear inequalities, find a solution.
ILP. Given a system of linear inequalities, find a binary solution.

Q. Which of these problems have poly-time solutions?
A. No easy answers.

√ LSOLVE. Yes. Gaussian elimination solves N-by-N system in N^3 time.
√ LP. Yes. Celebrated ellipsoid algorithm is poly-time.
? ILP. No poly-time algorithm known or believed to exist!

Search Problems

or report none exists

Search problem. Given an instance I of a problem, find a solution S.
Requirement. Must be able to efficiently check that S is a solution.

poly-time in size of instance I

Search Problems

or report none exists

Search problem. Given an instance I of a problem, find a solution S.
Requirement. Must be able to efficiently check that S is a solution.

poly-time in size of instance I

LSOLVE. Given a system of linear equations, find a solution.

$$\begin{array}{rrrcr} 0x_0 & + 1x_1 & + 1x_2 & = & 4 \\ 2x_0 & + 4x_1 & - 2x_2 & = & 2 \\ 0x_0 & + 3x_1 & + 15x_2 & = & 36 \end{array} \qquad \begin{array}{rcr} x_0 & = & -1 \\ x_1 & = & 2 \\ x_2 & = & 2 \end{array}$$

instance I   solution S

- To check solution S, plug in values and verify each equation.

Search Problems

or report none exists

Search problem. Given an instance I of a problem, find a solution S.
Requirement. Must be able to efficiently check that S is a solution.

poly-time in size of instance I

LP. Given a system of linear inequalities, find a solution.

$$\begin{array}{rcrcrcl} 48x_0 & + & 16x_1 & + & 119x_2 & \le & 88 \\ 5x_0 & + & 4x_1 & + & 35x_2 & \ge & 13 \\ 15x_0 & + & 4x_1 & + & 20x_2 & \ge & 23 \\ x_0 & , & x_1 & , & x_2 & \ge & 0 \end{array}$$

instance I

$$\begin{array}{rcl} x_0 & = & 1 \\ x_1 & = & 1 \\ x_2 & = & 1/5 \end{array}$$

solution S

- To check solution S, plug in values and verify each inequality.

NP

can check proposed solution in poly-time

Def. NP † is the class of all search problems.

† slightly non-standard definition

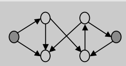
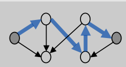
Problem	Description	Poly-time algorithm	Instance	Solution
LSOLVE (A, b)	Find a vector x that satisfies Ax = b.	Gaussian elimination	$0x_0 + 1x_1 + 1x_2 = 4$ $2x_0 + 4x_1 - 2x_2 = 2$ $0x_0 + 3x_1 + 15x_2 = 36$	$x_0 = -1$ $x_1 = 2$ $x_2 = 2$
LP (A, b)	Find a vector x that satisfies Ax ≤ b.	ellipsoid	$48x_0 + 16x_1 + 119x_2 \le 88$ $5x_0 + 4x_1 + 35x_2 \ge 13$ $15x_0 + 4x_1 + 20x_2 \ge 23$ $x_0 , x_1 , x_2 \ge 0$	$x_0 = 1$ $x_1 = 1$ $x_2 = 1/5$
ILP (A, b)	Find a binary vector x that satisfies Ax ≤ b.	???	$x_1 + x_2 \ge 1$ $x_0 + x_2 \ge 1$ $x_0 + x_1 + x_2 \le 2$	$x_0 = 0$ $x_1 = 1$ $x_2 = 1$
FACTOR (x)	Find a nontrivial factor of the integer x.	???	8784561	8243 × 10657

Significance. What scientists and engineers aspire to compute feasibly.

P

Def. P † is the class of search problem solvable in poly-time.

† slightly non-standard definition

Problem	Description	Poly-time algorithm	Instance	Solution
STCONN (G, s, t)	Find a path from s to t in digraph G.	depth-first search (Theseus)		
SORT (a)	Find permutation that puts a in ascending order.	mergesort (von Neumann 1945)	2.3 8.5 1.2 9.1 2.2 0.3	5 2 4 0 1 3
LSOLVE (A, b)	Find a vector x that satisfies Ax = b.	Gaussian elimination (Edmonds, 1967)	$0x_0 + 1x_1 + 1x_2 = 4$ $2x_0 + 4x_1 - 2x_2 = 2$ $0x_0 + 3x_1 + 15x_2 = 36$	$x_0 = -1$ $x_1 = 2$ $x_2 = 2$
LP (A, b)	Find a vector x that satisfies Ax ≤ b.	ellipsoid (Khachiyan, 1979)	$48x_0 + 16x_1 + 119x_2 \le 88$ $5x_0 + 4x_1 + 35x_2 \ge 13$ $15x_0 + 4x_1 + 20x_2 \ge 23$ $x_0 , x_1 , x_2 \ge 0$	$x_0 = 1$ $x_1 = 1$ $x_2 = 1/5$

Significance. What scientists and engineers compute feasibly.

Extended Church-Turing Thesis

Extended Church-Turing thesis.

P = search problem solvable in poly-time in this universe.

Evidence supporting thesis. True for all physical computers.

Implication. To make future computers more efficient,
suffices to focus on improving implementation of existing designs.

A new law of physics? A constraint on what is possible.
Possible counterexample? Quantum computers.

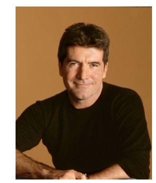
P vs. NP

Automating Creativity

Q. Being creative vs. appreciating creativity?

Ex. Mozart composes a piece of music; our neurons appreciate it.
Ex. Wiles proves a deep theorem; a colleague referees it.
Ex. Boeing designs an efficient airfoil; a simulator verifies it.
Ex. Einstein proposes a theory; an experimentalist validates it.

creative



ordinary

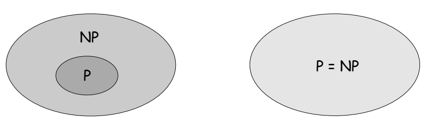
Computational analog. Does P = NP?

The Central Question

P. Class of search problem solvable in poly-time.
NP. Class of all search problems.

Does P = NP? [Is checking a solution as easy as finding one?]

Two worlds.



P ≠ NP   P = NP

If yes… Poly-time algorithms for 3-SAT, ILP, TSP, FACTOR, …
If no… Would learn something fundamental about our universe.

Overwhelming consensus. P ≠ NP.

Classifying Problems

A Hard Problem: 3-Satisfiability

Literal. A Boolean variable or its negation. x_i or $\overline{x_i}$

Clause. A disjunction of 3 distinct literals. $C_j = x_1 \vee \overline{x_2} \vee x_3$

Conjunctive normal form. A propositional formula that is the conjunction of clauses. $\Phi = C_1 \wedge C_2 \wedge C_3 \wedge C_4$

3-SAT. Given a CNF formula Φ consisting of k clauses over n literals, find a satisfying truth assignment (if one exists).

$$\Phi = \left(\overline{x_1} \vee x_2 \vee x_3\right) \wedge \left(x_1 \vee \overline{x_2} \vee x_3\right) \wedge \left(\overline{x_1} \vee \overline{x_2} \vee \overline{x_3}\right) \wedge \left(\overline{x_1} \vee \overline{x_2} \vee x_4\right)$$

Solution: $x_1 = \text{true}, \; x_2 = \text{true}, \; x_3 = \text{false}, \; x_4 = \text{true}$

Key application. Electronic design automation (EDA).

Exhaustive Search

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"

Classifying Problems

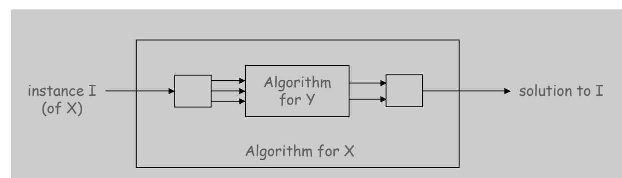
Q. Which search problems are in P?
A. No easy answers (we don't even know whether P = NP).

Goal. Formalize notion:

Problem X is computationally not much harder than problem Y.

Reductions

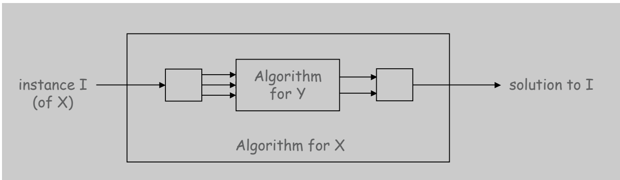
Def. Problem X reduces to problem Y if you can solve X given:
- A poly number of standard computational steps, plus
- A poly number of calls to a subroutine for solving instances of Y.



Reductions: Consequences

Def. Problem X reduces to problem Y if you can solve X given:

- A poly number of standard computational steps, plus
- A poly number of calls to a subroutine for solving instances of Y.



previously solved problem your research problem

Design algorithms. If poly-time algorithm for Y, then one for X too.
Establish intractability. If no poly-time algorithm for X, then none for Y.

3-SAT your research problem

LSOLVE Reduces to LP

LSOLVE. Given a system of linear equations Ax = b, find a solution x.

$$\begin{array}{rcrcrcr} 0x_0 & + & 1x_1 & + & 1x_2 & = & 4 \\ 2x_0 & + & 4x_1 & - & 2x_2 & = & 2 \\ 0x_0 & + & 3x_1 & + & 15x_2 & = & 36 \end{array}$$

LSOLVE instance with n variables

LP. Given a system of linear inequalities Ax ≤ b, find a solution x.

$$\left.\begin{array}{rcrcrcr} 0x_0 & + & 1x_1 & + & 1x_2 & \le & 4 \\ 0x_0 & - & 1x_1 & - & 1x_2 & \le & -4 \end{array}\right\} \Rightarrow 0x_0 + 1x_1 + 1x_1 = 4$$

$$\begin{array}{rcrcrcr} 2x_0 & + & 4x_1 & - & 2x_2 & \le & 2 \\ -2x_0 & - & 4x_1 & + & 2x_2 & \le & -2 \\ 0x_0 & + & 3x_1 & + & 15x_2 & \le & 36 \\ 0x_0 & - & 3x_1 & - & 15x_2 & \le & -36 \end{array}$$

corresponding LP instance with n variables and 2n inequalities

3-SAT Reduces to ILP

3-SAT. Given a CNF formula Φ, find a satisfying truth assignment.

$$\Phi = (\overline{x_1} \lor x_2 \lor x_3) \land (x_1 \lor \overline{x_2} \lor x_3) \land (\overline{x_1} \lor \overline{x_2} \lor \overline{x_3}) \land (\overline{x_1} \lor \overline{x_2} \lor x_4)$$

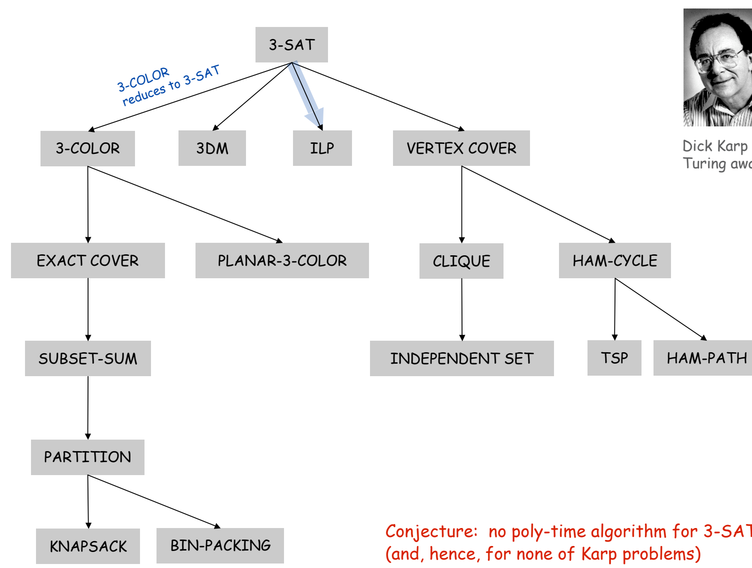
3-SAT instance with n variables, k clauses

ILP. Given a system of linear inequalities, find a binary solution.

$$\underbrace{\begin{array}{lcl} C_1 & \ge & 1 - x_1 \\ C_1 & \ge & x_2 \\ C_1 & \ge & x_3 \\ C_1 & \le & (1 - x_1) + x_2 + x_3 \end{array}}_{\Rightarrow\ C_1 = 1 \text{ iff clause 1 is satisfied}} \qquad \underbrace{\begin{array}{lcl} \Phi & \le & C_1 \\ \Phi & \le & C_2 \\ \Phi & \le & C_3 \\ \Phi & \le & C_4 \\ \Phi & \ge & C_1 + C_2 + C_3 + C_4 - 3 \end{array}}_{\Rightarrow\ \Phi = 1 \text{ iff } C_1 = C_2 = C_3 = C_4 = 1}$$

corresponding ILP instance with n+k+1 variables and 4k + k + 1 inequalities

More Reductions From 3-SAT



Dick Karp
Turing award (1985)

Conjecture: no poly-time algorithm for 3-SAT.
(and, hence, for none of Karp problems)

Still More Reductions from 3-SAT

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.
Medicine. Reconstructing 3d shape from biplane angiocardiogram.
Operations research. Traveling salesperson problem, integer programming.
Physics. Partition function of 3d Ising model.
Politics. Shapley-Shubik voting power.
Pop culture. Versions of Sudoko, Checkers, Minesweeper, Tetris.
Statistics. Optimal experimental design.

6,000+ scientific papers per year.

NP-Completeness

NP-Completeness

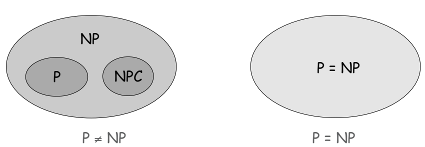
Q. Why do we believe 3-SAT has no poly-time algorithm?

Def. An NP problem is NP-complete if all problems in NP reduce to it.

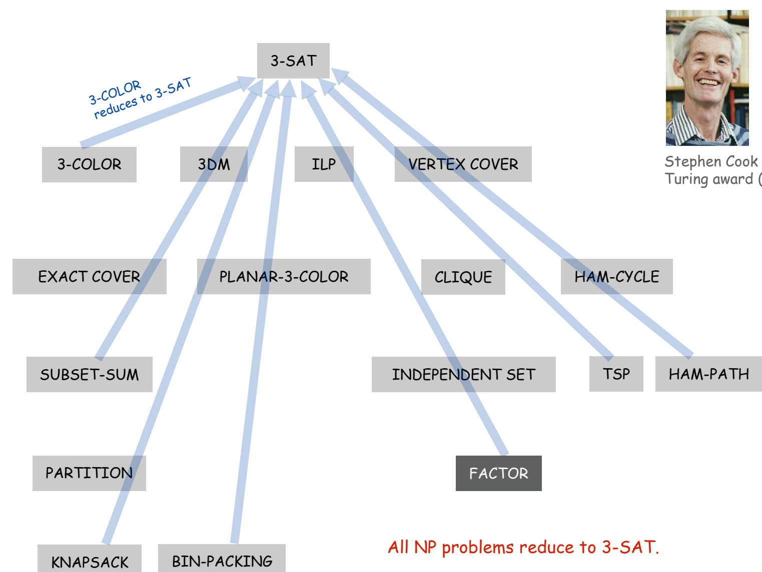
every NP problem is a 3-SAT problem in disguise

Theorem. [Cook 1961] 3-SAT is NP-complete.
Corollary. Poly-time algorithm for 3-SAT ⇒ P = NP.

Two worlds.



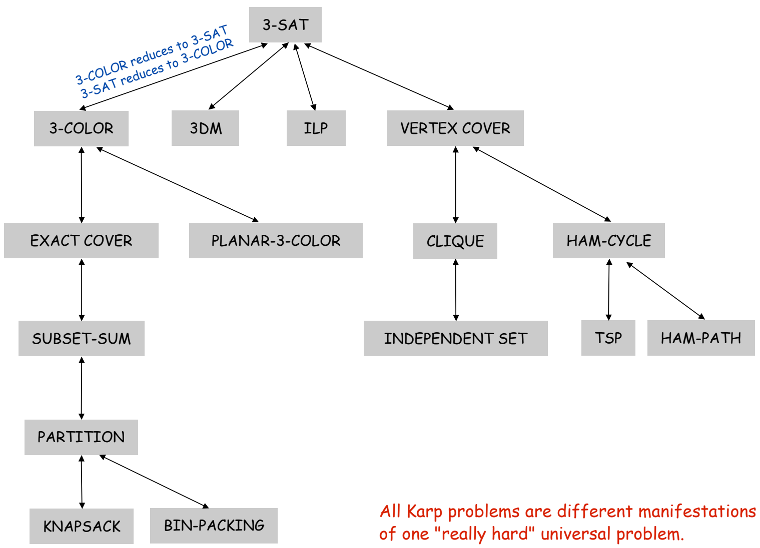
Cook's Theorem



Stephen Cook
Turing award (1982)

All NP problems reduce to 3-SAT.

Cook + Karp



All Karp problems are different manifestations of one "really hard" universal problem.

Implications of NP-Completeness

Implication. [3-SAT captures difficulty of whole class NP.]

- Poly-time algorithm for 3-SAT iff P = NP.
- If no poly-time algorithm for some NP problem, then none for 3-SAT.

Remark. Can replace 3-SAT with any of Karp's problems.

Proving a problem intractable guides scientific inquiry.

- 1926: Ising introduces simple model for phase transitions.
- 1944: Onsager finds closed form solution to 2d version in tour de force.
- 19xx: Feynman and other top minds seek 3d solution.
- 2000: 3-SAT reduces to 3D-ISING.

a holy grail of statistical mechanics

search for closed formula appears doomed

Coping with Intractability

Coping With Intractability

Relax one of desired features.

- Solve the problem in poly-time.
- Solve the problem to optimality.
- Solve arbitrary instances of the problem.

Complexity theory deals with worst case behavior.

- Instance(s) you want to solve may be "easy."
- `Chaff` solves real-world SAT instances with ~ 10k variable. [Matthew Moskewicz '00, Conor Madigan '00, Sharad Malik]

PU senior independent work (!)

Coping With Intractability

Relax one of desired features.

- Solve the problem in poly-time.
- Solve the problem to optimality.
- Solve arbitrary instances of the problem.

Develop a heuristic, and hope it produces a good solution.

- No guarantees on quality of solution.
- Ex. TSP assignment heuristics.
- Ex. Metropolis algorithm, simulating annealing, genetic algorithms.

Approximation algorithm. Find solution of provably good quality.

- Ex. MAX-3SAT: provably satisfy 87.5% as many clauses as possible.

but if you can guarantee to satisfy 87.51% as many clauses as possible in poly-time, then P = NP !

Coping With Intractability

Relax one of desired features.

- Solve the problem in poly-time.
- Solve the problem to optimality.
- Solve arbitrary instances of the problem.

Special cases may be tractable.

- Ex: Linear time algorithm for 2-SAT.
- Ex: Linear time algorithm for Horn-SAT.

each clause has at most one un-negated literal

Exploiting Intractability: Cryptography

Modern cryptography.

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

RSA cryptosystem.

- To use: multiply two n-bit integers. [poly-time]
- To break: factor a 2n-bit integer. [unlikely poly-time]

Multiply = EASY

$$23 \times 67 \rightleftarrows 1{,}541$$

Factor = HARD

Exploiting Intractability: Cryptography

FACTOR. Given an n-bit integer x, find a nontrivial factor.

not 1 or x

```
74037563479561712828046796097429573142593188889231289
08493623263897276503402826627689199641962511784399589
43305021275853701189680982867331732731089309005525051
16877063299072396380786710086096962537934650563796359
```

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

Exploiting Intractability: Cryptography

FACTOR. Given an n-bit integer x, find a nontrivial factor.

not 1 or x

Q. What is complexity of FACTOR?
A. In NP, but not known (or believed) to be in P or NP-complete.

Q. What if P = NP?
A. Poly-time algorithm for factoring; modern e-conomy collapses.

Quantum. [Shor 1994] Can factor an n-bit integer in n^3 steps on a "quantum computer."

Summary

P. Class of search problems solvable in poly-time.
NP. Class of search problems, some of which seem wickedly hard.
NP-complete. Hardest problems in NP.

Many fundamental problems are intractable.

- TSP, 3-SAT, 3-COLOR, ILP.
- 3D-ISING.

Theory says: we probably can't design efficient algorithms for them.

- You will confront NP-complete problems in your career.
- So, identify these situations and proceed accordingly.