**AAVANCED TOPICS**

**Jun. 6, 2013**

Acknowledgement: The course slides are adapted from the slides prepared by R. Sedgewick and K. Wayne of Princeton University.

**Bird’s-eye view**

**Desiderata.** Classify problems according to computational requirements.

<table>
<thead>
<tr>
<th>Complexity</th>
<th>Order of Growth</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linear</td>
<td>$N$</td>
<td>min, max, median, Burrows-Wheeler transform, ...</td>
</tr>
<tr>
<td>Linearithmic</td>
<td>$N \log N$</td>
<td>sorting, convex hull, closest pair, farthest pair, ...</td>
</tr>
<tr>
<td>Quadratic</td>
<td>$N^2$</td>
<td>?</td>
</tr>
<tr>
<td>Exponential</td>
<td>$c^n$</td>
<td>?</td>
</tr>
</tbody>
</table>

**Frustrating news.** Huge number of problems have defied classification.

**Bird’s-eye view**

**Desiderata.** Classify problems according to computational requirements.

**Desiderata’.**
Suppose we could (could not) solve problem $X$ efficiently. What else could (could not) we solve efficiently?

"Give me a lever long enough and a fulcrum on which to place it, and I shall move the world." — Archimedes
Reduction

Def. Problem $X$ reduces to problem $Y$ if you can use an algorithm that solves $Y$ to help solve $X$.

Ex 1. [element distinctness reduces to sorting]
To solve element distinctness on $N$ items:
- Sort $N$ items.
- Check adjacent pairs for equality.

Cost of solving element distinctness. $N \log N + N$.

Ex 2. [3-collinear reduces to sorting]
To solve 3-collinear instance on $N$ points in the plane:
- For each point, sort other points by polar angle or slope.
  - check adjacent triples for collinearity

Cost of solving 3-collinear. $N^2 \log N + N^2$. 

Reduction

Def. Problem $X$ reduces to problem $Y$ if you can use an algorithm that solves $Y$ to help solve $X$.

Ex 1. [element distinctness reduces to sorting]
To solve element distinctness on $N$ items:
- Sort $N$ items.
- Check adjacent pairs for equality.

Cost of solving element distinctness. $N \log N + N$.

Ex 2. [3-collinear reduces to sorting]
To solve 3-collinear instance on $N$ points in the plane:
- For each point, sort other points by polar angle or slope.
  - check adjacent triples for collinearity

Cost of solving 3-collinear. $N^2 \log N + N^2$. 

Reductions

- Designing algorithms
- Establishing lower bounds
- Classifying problems
Reduction: design algorithms

Def. Problem $X$ reduces to problem $Y$ if you can use an algorithm that solves $Y$ to help solve $X$.

Design algorithm. Given algorithm for $Y$, can also solve $X$.

Ex.
- Element distinctness reduces to sorting.
- 3-collinear reduces to sorting.
- CPM reduces to topological sort. [shortest paths lecture]
- h-v line intersection reduces to 1d range searching. [geometric BST lecture]
- Baseball elimination reduces to maxflow. [assignment 7]
- Burrows-Wheeler transform reduces to suffix sort. [assignment 8]
- ...

Mentality. Since I know how to solve $Y$, can I use that algorithm to solve $X$?

programmer’s version: I have code for $Y$. Can I use it for $X$?

Convex hull reduces to sorting

Sorting. Given $N$ distinct integers, rearrange them in ascending order.

Convex hull. Given $N$ points in the plane, identify the extreme points of the convex hull (in counterclockwise order).

Convex hull reduces to sorting

Cost of convex hull. $N \log N + N$.

Graham scan algorithm

Graham scan.
- Choose point $p$ with smallest (or largest) y-coordinate.
- Sort points by polar angle with $p$ to get simple polygon.
- Consider points in order, and discard those that would create a clockwise turn.

Shortest paths on edge-weighted graphs and digraphs

Proposition. Undirected shortest paths (with nonnegative weights) reduces to directed shortest path.
Shortest paths on edge-weighted graphs and digraphs

**Proposition.** Undirected shortest paths (with nonnegative weights) reduces to directed shortest path.

**Pf.** Replace each undirected edge by two directed edges.

Cost of undirected shortest paths. \( E \log V + E. \)

Shortest paths with negative weights

**Caveat.** Reduction is invalid for edge-weighted graphs with negative weights (even if no negative cycles).

**Remark.** Can still solve shortest-paths problem in undirected graphs (if no negative cycles), but need more sophisticated techniques.

Some reductions involving familiar problems
**Reductions**

- Designing algorithms
- Establishing lower bounds
- Classifying problems

---

**Bird’s-eye view**

**Goal.** Prove that a problem requires a certain number of steps.

**Ex.** In decision tree model, any compare-based sorting algorithm requires \( \Omega(N \log N) \) compares in the worst case.

**Bad news.** Very difficult to establish lower bounds from scratch.

**Good news.** Spread \( \Omega(N \log N) \) lower bound to \( Y \) by reducing sorting to \( Y \).

assuming cost of reduction is not too high

---

**Element distinctness linear-time reduces to closest pair**

**Closest pair.** Given \( N \) points in the plane, find the closest pair.

**Element distinctness.** Given \( N \) elements, are any two equal?

**Proposition.** Element distinctness linear-time reduces to closest pair:

**Pf.**
- Element distinctness instance: \( x_1, x_2, \ldots, x_N \).
- Closest pair instance: \((x_1, x_1), (x_2, x_2), \ldots, (x_N, x_N)\).
- Two elements are distinct if and only if closest pair = 0.

allows quadratic tests of the form: \( x_i < x_j \) or \( (x_i - x_j)^2 - (x_k - x_l)^2 < 0 \)

**Element distinctness lower bound.** In quadratic decision tree model, any algorithm that solves element distinctness takes \( \Omega(N \log N) \) steps.

**Implication.** In quadratic decision tree model, any algorithm for closest pair takes \( \Omega(N \log N) \) steps.

---

**Linear-time reductions**

**Def.** Problem \( X \) linear-time reduces to problem \( Y \) if \( X \) can be solved with:
- Linear number of standard computational steps.
- Constant number of calls to \( Y \).

**Ex.** Almost all of the reductions we’ve seen so far. [Which ones weren’t?]

**Establish lower bound:**
- If \( X \) takes \( \Omega(N \log N) \) steps, then so does \( Y \).
- If \( X \) takes \( \Omega(N^2) \) steps, then so does \( Y \).

**Mentality.**
- If I could easily solve \( Y \), then I could easily solve \( X \).
- I can’t easily solve \( X \).
- Therefore, I can’t easily solve \( Y \).
More linear-time reductions and lower bounds

Establishing lower bounds: summary

Establishing lower bounds through reduction is an important tool in guiding algorithm design efforts.

Q. How to convince yourself no linear-time convex hull algorithm exists?
A2. [easy way] Linear-time reduction from sorting.

Classifying problems: summary

Desiderata. Problem with algorithm that matches lower bound.
Ex. Sorting, convex hull, and closest pair have complexity \( N \log N \).

Desiderata'. Prove that two problems \( X \) and \( Y \) have the same complexity.
• First, show that problem \( X \) linear-time reduces to \( Y \).
• Second, show that \( Y \) linear-time reduces to \( X \).
• Conclude that \( X \) and \( Y \) have the same complexity.

even if we don’t know what it is!
Caveat

**SORT.** Given \( N \) distinct integers, rearrange them in ascending order.

**CONVEX HULL.** Given \( N \) points in the plane, identify the extreme points of the convex hull (in counterclockwise order).

**Proposition.** \( \text{SORT} \) linear-time reduces to \( \text{CONVEX HULL} \).
**Proposition.** \( \text{CONVEX HULL} \) linear-time reduces to \( \text{SORT} \).
**Conclusion.** \( \text{SORT} \) and \( \text{CONVEX HULL} \) have the same complexity.

A possible real-world scenario.
- System designer specs the APIs for project.
- Alice implements \texttt{sort()} using \texttt{convexHull()}.
- Bob implements \texttt{convexHull()} using \texttt{sort}().
- Infinite reduction loop!
- Who’s fault?

Integer arithmetic reductions

**Integer multiplication.** Given two \( N \)-bit integers, compute their product.
**Brute force.** \( N^2 \) bit operations.

<table>
<thead>
<tr>
<th>problem</th>
<th>arithmetic</th>
<th>order of growth</th>
</tr>
</thead>
<tbody>
<tr>
<td>integer multiplication</td>
<td>( a \times b )</td>
<td>( M(N) )</td>
</tr>
<tr>
<td>integer division</td>
<td>( a / b, a \mod b )</td>
<td>( M(N) )</td>
</tr>
<tr>
<td>integer square</td>
<td>( a^2 )</td>
<td>( M(N) )</td>
</tr>
<tr>
<td>integer square root</td>
<td>( \lfloor \sqrt{a} \rfloor )</td>
<td>( M(N) )</td>
</tr>
</tbody>
</table>

integer arithmetic problems with the same complexity as integer multiplication

**Q.** Is brute-force algorithm optimal?

History of complexity of integer multiplication

<table>
<thead>
<tr>
<th>year</th>
<th>algorithm</th>
<th>order of growth</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>brute force</td>
<td>( N^2 )</td>
</tr>
<tr>
<td>1962</td>
<td>Karatsuba-Ofman</td>
<td>( N^{1.585} )</td>
</tr>
<tr>
<td>1963</td>
<td>Toom-3, Toom-4</td>
<td>( N^{1.465} ), ( N^{1.404} )</td>
</tr>
<tr>
<td>1966</td>
<td>Toom-Cook</td>
<td>( N + \varepsilon )</td>
</tr>
<tr>
<td>1971</td>
<td>Schönhage-Strassen</td>
<td>( N \log N \log \log N )</td>
</tr>
<tr>
<td>2007</td>
<td>Fürer</td>
<td>( N \log N^2 \log N )</td>
</tr>
<tr>
<td>?</td>
<td>?</td>
<td>( N )</td>
</tr>
</tbody>
</table>

number of bit operations to multiply two \( N \)-bit integers

**Remark.** GNU Multiple Precision Library uses one of five different algorithm depending on size of operands.
### Linear algebra reductions

**Matrix multiplication.** Given two \( N \)-by-\( N \) matrices, compute their product.

**Brute force.** \( N^3 \) flops.

\[
\begin{pmatrix}
0.1 & 0.2 & 0.8 & 0.1 \\
0.5 & 0.3 & 0.9 & 0.6 \\
0.1 & 0.0 & 0.7 & 0.4 \\
0.0 & 0.3 & 0.3 & 0.1
\end{pmatrix}
\times
\begin{pmatrix}
0.4 & 0.3 & 0.1 & 0.1 \\
0.2 & 0.2 & 0.0 & 0.6 \\
0.0 & 0.0 & 0.4 & 0.5 \\
0.8 & 0.4 & 0.1 & 0.9
\end{pmatrix}
= \\
\begin{pmatrix}
0.16 & 0.11 & 0.34 & 0.62 \\
0.74 & 0.45 & 0.47 & 1.22 \\
0.36 & 0.19 & 0.33 & 0.72 \\
0.14 & 0.10 & 0.13 & 0.42
\end{pmatrix}
\]

\[
0.5 \cdot 0.1 + 0.3 \cdot 0.0 + 0.9 \cdot 0.4 + 0.6 \cdot 0.1 = 0.47
\]

**Q.** Is brute-force algorithm optimal?

### History of complexity of matrix multiplication

<table>
<thead>
<tr>
<th>year</th>
<th>algorithm</th>
<th>order of growth</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>brute force</td>
<td>( N^3 )</td>
</tr>
<tr>
<td>1969</td>
<td>Strassen</td>
<td>( N^{1.808} )</td>
</tr>
<tr>
<td>1978</td>
<td>Pan</td>
<td>( N^{2.276} )</td>
</tr>
<tr>
<td>1979</td>
<td>Bini</td>
<td>( N^{2.380} )</td>
</tr>
<tr>
<td>1981</td>
<td>Schönhage</td>
<td>( N^{2.322} )</td>
</tr>
<tr>
<td>1982</td>
<td>Romani</td>
<td>( N^{2.317} )</td>
</tr>
<tr>
<td>1982</td>
<td>Coppersmith-Winograd</td>
<td>( N^{2.396} )</td>
</tr>
<tr>
<td>1986</td>
<td>Strassen</td>
<td>( N^{2.479} )</td>
</tr>
<tr>
<td>1989</td>
<td>Coppersmith-Winograd</td>
<td>( N^{2.376} )</td>
</tr>
<tr>
<td>2010</td>
<td>Strother</td>
<td>( N^{2.377} )</td>
</tr>
<tr>
<td>2011</td>
<td>Williams</td>
<td>( N^{2.377} )</td>
</tr>
<tr>
<td>?</td>
<td></td>
<td>( N^{2 + \varepsilon} )</td>
</tr>
</tbody>
</table>

### Birds-eye view: revised

**Desiderata.** Classify problems according to computational requirements.

<table>
<thead>
<tr>
<th>complexity</th>
<th>order of growth</th>
<th>examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>linear</td>
<td>( N )</td>
<td>min, max, median, \ldots</td>
</tr>
<tr>
<td>linearithmic</td>
<td>( N \log N )</td>
<td>sorting, convex hull, closest pair, farthest pair, \ldots</td>
</tr>
<tr>
<td>( M(N) )</td>
<td>( ? )</td>
<td>integer multiplication, division, square root, \ldots</td>
</tr>
<tr>
<td>( MM(N) )</td>
<td>( ? )</td>
<td>matrix multiplication, ( Ax = b ), least square, determinant, \ldots</td>
</tr>
<tr>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td>( \vdots )</td>
</tr>
<tr>
<td>( \vdots )</td>
<td>( \vdots )</td>
<td>( \vdots )</td>
</tr>
<tr>
<td>( NP-complete )</td>
<td>probably not ( N^k )</td>
<td>3-SAT, IND-SET, ILP, \ldots</td>
</tr>
</tbody>
</table>

**Good news.** Can put many problems into equivalence classes.
Summary

Reductions are important in theory to:
- Establish tractability.
- Establish intractability.
- Classify problems according to their computational requirements.

Reductions are important in practice to:
- Design algorithms.
- Design reusable software modules.
  - stacks, queues, priority queues, symbol tables, sets, graphs
  - sorting, regular expressions, Delaunay triangulation
  - MST, shortest path, maxflow, linear programming
- Determine difficulty of your problem and choose the right tool.
  - use exact algorithm for tractable problems
  - use heuristics for intractable problems

Questions about computation

Q. What is a general-purpose computer?
Q. Are there limits on the power of digital computers?
Q. Are there limits on the power of machines we can build?

A simple model of computation: DFAs

Tape.
- Stores input.
- One arbitrarily long strip, divided into cells.
- Finite alphabet of symbols.

Tape head.
- Points to one cell of tape.
- Reads a symbol from active cell.
- Moves one cell at a time.

Q. Is there a more powerful model of computation?
A. Yes.
A universal model of computation: Turing machines

Tape.
- Stores input, output, and intermediate results.
- One arbitrarily long strip, divided into cells.
- Finite alphabet of symbols.

Tape head.
- Points to one cell of tape.
- Reads a symbol from active cell.
- Writes a symbol to active cell.
- Moves one cell at a time.

Q. Is there a more powerful model of computation?
A. No! — most important scientific result of 20th century?

Church-Turing thesis (1936)

Turing machines can compute any function that can be computed by a physically harnessable process of the natural world.

Remark. "Thesis" and not a mathematical theorem because it’s a statement about the physical world and not subject to proof.

Use simulation to prove models equivalent.
- Android simulator on iPhone.
- iPhone simulator on Android.

Implications.
- No need to seek more powerful machines or languages.
- Enables rigorous study of computation (in this universe).

Bottom line. Turing machine is a simple and universal model of computation.

A question about algorithms

Q. Which algorithms are useful in practice?
- Measure running time as a function of input size \( N \).
- Useful in practice ("efficient") = polynomial time for all inputs.

Ex 1. Sorting \( N \) items takes \( N \log N \) compares using mergesort.
Ex 2. Finding best TSP tour on \( N \) points takes \( N! \) steps using brute search.

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

<table>
<thead>
<tr>
<th>model of computation</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enhanced Turing machines</td>
<td>multiple heads, multiple tapes, 2D tape, nondeterminism</td>
</tr>
<tr>
<td>untyped lambda calculus</td>
<td>method to define and manipulate functions</td>
</tr>
<tr>
<td>recursive functions</td>
<td>functions dealing with computation on integers</td>
</tr>
<tr>
<td>unrestricted grammars</td>
<td>iterative string replacement rules used by linguists</td>
</tr>
<tr>
<td>extended L-systems</td>
<td>parallel string replacement rules that model plant growth</td>
</tr>
<tr>
<td>programming languages</td>
<td>Java, C, C++, Perl, Python, PHP, Lisp, PostScript, Excel</td>
</tr>
<tr>
<td>random access machines</td>
<td>registers plus main memory, e.g., TOY, Pentium</td>
</tr>
<tr>
<td>cellular automata</td>
<td>cells which change state based on local interactions</td>
</tr>
<tr>
<td>quantum computer</td>
<td>compute using superposition of quantum states</td>
</tr>
<tr>
<td>DNA computer</td>
<td>compute using biological operations on DNA</td>
</tr>
</tbody>
</table>

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...

\[ 1000! >> 10^{70} >> 10^{79} \times 10^{13} \times 10^{17} \]

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

Questions about problems

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

Q. Which problems have poly-time algorithms?
A. Not so easy to know. Focus of today’s lecture.

Bird’s-eye view

Def. A problem is intractable if it can’t be solved in polynomial time.

Desiderata. Prove that a problem is intractable.

Two problems that provably require exponential time.

- Given a constant-size program, does it halt in at most \( K \) steps?
- Given \( N \)-by-\( N \) checkers board position, can the first player force a win?

Frustrating news. Very few successes.

INTRACTABILITY

- Search problems
- P vs. NP
- Classifying problems
- NP-completeness
Four fundamental problems

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

\[
\begin{align*}
0x_0 + 1x_1 + 1x_2 &= 4 \\
2x_0 + 4x_1 - 2x_2 &= 2 \\
0x_0 + 3x_1 + 15x_2 &= 36
\end{align*}
\]

 variables are real numbers

\[
\begin{align*}
x_0 &= -1 \\
x_1 &= 2 \\
x_2 &= 2
\end{align*}
\]

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

\[
\begin{align*}
4x_0 + 16x_1 + 19x_2 &\leq 88 \\
5x_0 + 4x_1 + 35x_2 &\geq 13 \\
15x_0 + 4x_1 + 20x_2 &\geq 23 \\
x_2 &\geq 0
\end{align*}
\]

 variables are real numbers

\[
\begin{align*}
x_0 &= 1 \\
x_1 &= 1 \\
x_2 &= 1
\end{align*}
\]

**ILP.** Given a system of **linear inequalities**, find a 0-1 solution.

\[
\begin{align*}
x_1 + x_2 &\geq 1 \\
x_0 + x_2 &\geq 1 \\
x_0 + x_1 + x_2 &\leq 2
\end{align*}
\]

 variables are 0 or 1

\[
\begin{align*}
x_0 &= 0 \\
x_1 &= 1 \\
x_2 &= 1
\end{align*}
\]

**SAT.** Given a system of **boolean equations**, find a binary solution.

\[
\begin{align*}
(x_1 \lor x_2) \land (x_0 \lor x_1) &= \text{true} \\
(x_0 \lor x_2) \land (x_0 \lor x_2) &= \text{true} \\
(x_0 \lor x_1) \land (x_1 \lor x_2) &= \text{true} \\
(x_0 \lor x_2) \land (x_0 \lor x_2) &= \text{false}
\end{align*}
\]

 variables are true or false

\[
\begin{align*}
x_0 &= \text{false} \\
x_1 &= \text{false} \\
x_2 &= \text{true}
\end{align*}
\]

Search problems

**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.

or report none exists

poly-time in size of instance \(I\)

To check solution \(S\), plug in values and verify each equation.

---

Q. Which of these problems have poly-time algorithms?

- **LSOLVE.** Yes. Gaussian elimination solves \(N\)-by-\(N\) system in \(N^3\) time.
- **LP.** Yes. Ellipsoid elimination is poly-time. But was open problem for decades.
- **ILP, SAT.** No poly-time algorithm known or believed to exist! But we still don’t know for sure.
Search problems

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.

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

\[
\begin{align*}
48x_0 + 16x_1 + 119x_2 & \leq 88 \\
5x_0 + 4x_1 + 35x_2 & \geq 13 \\
15x_0 + 4x_1 + 20x_2 & \geq 23 \\
x_0 + x_1 + x_2 & \geq 0
\end{align*}
\]

instance I

\[
\begin{align*}
x_0 &= 1 \\
x_1 &= 1 \\
x_2 &= \frac{1}{2}
\end{align*}
\]

solution S

To check solution \( S \), plug in values and verify each inequality.

SAT. Given a system of boolean equations, find a boolean solution.

\[
\begin{align*}
(x_1' \text{ or } x_2') \text{ and } (x_0 \text{ or } x_2) &= \text{true} \\
(x_0 \text{ or } x_1) \text{ and } (x_1' \text{ or } x_2') &= \text{false} \\
(x_0' \text{ or } x_2) \text{ and } (x_1') &= \text{true}
\end{align*}
\]

instance I

\[
\begin{align*}
x_0 &= \text{false} \\
x_1 &= \text{false} \\
x_2 &= \text{true}
\end{align*}
\]

solution S

To check solution \( S \), plug in values and verify each equation.

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

\[
\begin{align*}
147573952589676412927 \\
193707721
\end{align*}
\]

input size = number of bits

instance I

solution S

To check solution \( S \), long divide 193707721 into 147573952589676412927.
NP

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

Note: classic definition limits NP to yes-no problems

<table>
<thead>
<tr>
<th>problem</th>
<th>description</th>
<th>poly-time algorithm</th>
<th>instance I</th>
<th>solution S</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSOLVE</td>
<td>Find a vector ( x ) that satisfies ( Ax = b )</td>
<td>Gaussian elimination</td>
<td>( \begin{align*} 0x_0 + 1x_1 + 1x_2 &amp; = 4 \ 2x_0 + 4x_1 + 3x_2 &amp; = 2 \ 0x_0 + 3x_1 + 15x_2 &amp; = 36 \end{align*} )</td>
<td>( x_0 = -1, x_1 = 2, x_2 = 2 )</td>
</tr>
<tr>
<td>LP</td>
<td>Find a vector ( x ) that satisfies ( Ax \leq b )</td>
<td>ellipsoid</td>
<td>( \begin{align*} 4x_0 + 4x_1 + 11x_2 &amp; \leq 48 \ 2x_0 + 3x_1 &amp; \leq 15 \ 3x_0 + 4x_1 + 20x_2 &amp; \leq 25 \ x_0, x_1, x_2 &amp; \geq 0 \end{align*} )</td>
<td>( x_0 = 1, x_1 = 1, x_2 = \frac{5}{3} )</td>
</tr>
<tr>
<td>ILP</td>
<td>Find a binary vector ( x ) that satisfies ( Ax \leq b )</td>
<td>???</td>
<td>( x_0, x_1, x_2 )</td>
<td>( x_0 = 0, x_1 = 0, x_2 = 1 )</td>
</tr>
<tr>
<td>SAT</td>
<td>Find a boolean vector ( x ) that satisfies ( \Phi(x) = b )</td>
<td>???</td>
<td>???</td>
<td>???</td>
</tr>
<tr>
<td>FACTOR</td>
<td>Find a nontrivial factor of the integer ( x )</td>
<td>???</td>
<td>( 147573952589676412927 )</td>
<td>( 193707721 )</td>
</tr>
</tbody>
</table>

Significance. What scientists and engineers *aspire* to compute feasibly.

**NP-completeness**

- Search problems
- **P** vs. **NP**
- Classifying problems
- NP-completeness

**P**

Def. **P** is the class of search problems solvable in poly-time.

Note: classic definition limits P to yes-no problems

<table>
<thead>
<tr>
<th>problem</th>
<th>description</th>
<th>poly-time algorithm</th>
<th>instance I</th>
<th>solution S</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSOLVE</td>
<td>Find a vector ( x ) that satisfies ( Ax = b )</td>
<td>Gaussian elimination</td>
<td>( \begin{align*} 0x_0 + 1x_1 + 1x_2 &amp; = 4 \ 2x_0 + 4x_1 + 3x_2 &amp; = 2 \ 0x_0 + 3x_1 + 15x_2 &amp; = 36 \end{align*} )</td>
<td>( x_0 = -1, x_1 = 2, x_2 = 2 )</td>
</tr>
<tr>
<td>LP</td>
<td>Find a vector ( x ) that satisfies ( Ax \leq b )</td>
<td>ellipsoid</td>
<td>( \begin{align*} 4x_0 + 4x_1 + 11x_2 &amp; \leq 48 \ 2x_0 + 3x_1 &amp; \leq 15 \ 3x_0 + 4x_1 + 20x_2 &amp; \leq 25 \end{align*} )</td>
<td>( x_0 = 1, x_1 = 1, x_2 = \frac{5}{3} )</td>
</tr>
<tr>
<td>SORT</td>
<td>Find a permutation that puts array ( a ) in order</td>
<td>mergesort (von Neumann 1945)</td>
<td>( 2.385.12 )</td>
<td>( 5 2 4 0 1 3 )</td>
</tr>
<tr>
<td>STCONN</td>
<td>Find a path in a graph ( G ) from ( s ) to ( t )</td>
<td>depth-first search (Theseus)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Significance. What scientists and engineers *do* compute feasibly.

Non-deterministic machine can **guess** the desired solution.

Ex. int[] a = new int[N];  
Java: initializes entries to 0.  
Non-deterministic machine: initializes entries to the solution!

**ILP.** Given a system of linear inequalities, **guess** a 0-1 solution.

\[
\begin{align*}
  x_0 + x_1 & \geq 1 \\
  x_1 + x_2 & \geq 1 \\
  x_0 + x_1 + x_2 & \leq 2 
\end{align*}
\]

Ex. Turing machine.  
- Deterministic: state, input determines next state.  
- Non-deterministic: more than one possible next state.

**NP.** Search problems solvable in poly time on a non-deterministic TM.
**Extended Church-Turing thesis**

\[ P = \text{search problems solvable in poly-time in the natural world.} \]

**Evidence supporting thesis.** True for all physical computers.

**Natural computers?** No successful attempts (yet).

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

---

**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.

---

**P vs. NP**

**Does \( P = NP \)?**

---

**The central question**

**P.** Class of search problems solvable in poly-time.

**NP.** Class of all search problems.

**Does \( P = NP \)?** [Can you always avoid brute-force searching and do better]

**Two worlds.**

\[ \text{If } P = NP \ldots \text{ Poly-time algorithms for SAT, ILP, TSP, FACTOR, …} \]

\[ \text{If } P \neq NP \ldots \text{ Would learn something fundamental about our universe.} \]

**Overwhelming consensus.** \( P \neq NP \).
**The central question**

**P.** Class of search problems solvable in poly-time.

**NP.** Class of all search problems.

Does $P = NP$? [Can you always avoid brute-force searching and do better]

**Millennium prize.** $1$ million for resolution of $P = NP$ problem.

---

**A key problem: satisfiability**

**SAT.** Given a system of boolean equations, find a solution.

\[
\begin{align*}
x_1' \text{ or } x_2 \text{ or } x_3 &= \text{true} \\
x_1 \text{ or } x_2' \text{ or } x_3 &= \text{true} \\
x_1' \text{ or } x_2' \text{ or } x_3' &= \text{true} \\
x_1' \text{ or } x_2' \text{ or } x_4 &= \text{true}
\end{align*}
\]

**Key applications.**
- Automatic verification systems for software.
- Electronic design automation (EDA) for hardware.
- Mean field diluted spin glass model in physics.
- ...

---

**EXHAUSTIVE SEARCH**

**Q.** How to solve an instance of 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 SAT.

"intractable"
Classifying problems

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

Problem $X$ poly-time reduces to problem $Y$ if $X$ can be solved with:
- Polynomial number of standard computational steps.
- Polynomial number of calls to $Y$.

Consequence. If SAT poly-time reduces to $Y$, then we conclude that $Y$ is (probably) intractable.

SAT poly-time reduces to ILP

SAT. Given a system of boolean equations, find a solution.

1. $x_1 \lor x_2 \lor x_3 = \text{true}$
2. $x_1 \lor x_2' \lor x_3 = \text{true}$
3. $x_1' \lor x_2' \lor x_3 = \text{true}$
4. $x_1' \lor x_2' \lor x_4 = \text{true}$

can to reduce any SAT problem to this form

ILP. Given a system of linear inequalities, find a 0-1 solution.

1. $1 \leq (1 - x_1) + x_2 + x_3$
2. $1 \leq x_1 + (1 - x_2) + x_3$
3. $1 \leq (1 - x_1) + (1 - x_2) + (1 - x_3)$
4. $1 \leq (1 - x_1) + (1 - x_2) + x_4$

solution to this ILP instance gives solution to original SAT instance

More poly-time reductions from boolean satisfiability

SAT reduces to ILP

More poly-time reductions from boolean satisfiability

- SAT
- 3-COLOR
- IND-SET
- VERTEX COVER
- EXACT COVER
- CLIQUE
- HAM-CYCLE
- SUBSET-SUM
- ILP
- PARTITION
- KNAPSACK
- BIN-PACKING

Conjecture. SAT is intractable.
Implication. All of these problems are intractable.

Still more reductions from 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.
Game theory. Nash equilibrium that maximizes social welfare.
Mathematics. Given integer $a_1, \ldots, a_n$, compute $\prod_{i=1}^{n} \cos(a_i\phi) + \cos(a_i\delta)$
Mechanical engineering. Structure of turbulence in sheared flows.
Medicine. Reconstructing 3d shape from biplane angiogramgram.
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.

plus over 6,000 scientific papers per year
Intractability

- Search problems
- P vs. NP
- Classifying problems
- NP-completeness

NP-completeness

Definition. An NP problem is NP-complete if every problem in NP poly-time reduce to it.


Extremely brief proof sketch:
- Convert non-deterministic TM notation to SAT notation.
- If you can solve SAT, you can solve any problem in NP.

Corollary. Poly-time algorithm for SAT iff P = NP.

Implications of Cook-Levin theorem

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

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

Implications of NP-Completeness

Implication. [SAT captures difficulty of whole class NP]
- Poly-time algorithm for SAT iff $P = NP$.
- No poly-time algorithm for some NP problem $\Rightarrow$ none for SAT.

Remark. Can replace SAT with any of Karp’s problems.

Proving a problem NP-complete 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: 3D-ISING proved NP-complete.

Two worlds (more detail)

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

Summary

$P$. Class of search problems solvable in poly-time.
$NP$. Class of all search problems, some of which seem wickedly hard.
$NP$-complete. Hardest problems in $NP$.
Intractable. Problem with no poly-time algorithm.

Many fundamental problems are NP-complete.
- SAT, ILP, HAMILTON-PATH, …
- 3D-ISING, …

Use theory a guide:
- A poly-time algorithm for an NP-complete problem would be a stunning breakthrough (a proof that $P = NP$).
- You will confront NP-complete problems in your career.
- Safe to assume that $P \neq NP$ and that such problems are intractable.
- Identify these situations and proceed accordingly.
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 cryptosystem.
• To use: multiply two \( n \)-bit integers. [poly-time]
• To break: factor a 2 \( n \)-bit integer. [unlikely poly-time]

\[23 \times 67 \rightarrow 1,541\]

Factor = HARD

Multiply = EASY

Exploiting intractability

\textbf{FACTOR.} Given an \( n \)-bit integer \( x \), find a nontrivial factor.

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.

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

Q. Do we still believe the extended Church-Turing thesis???

Exploiting intractability

Challenge. Factor this number.

7403756347956171282804679609742957314259318888923132890849
362326389727650340282662768919964196251178439958943305021
2758537011896809828673311732731089309805525051168770632990
72396380786710086096962537934650563796359

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

Can’t do it? Create a company based on the difficulty of factoring.

Exploiting intractability

Relax one of desired features.
• Solve arbitrary instances of the problem.
• Solve the problem to optimality.
• Solve the problem in poly-time.

Special cases may be tractable.
• Ex: Linear time algorithm for 2-SAT. \rightarrow at most two variables per equation
• Ex: Linear time algorithm for Horn-SAT. \rightarrow at most one un-negated variable per equation

Coping with intractability
Coping with intractability

Relax one of desired features.
• Solve arbitrary instances of the problem.
• Solve the problem to optimality.
• Solve the problem in poly-time.

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 \( P = \text{NP} \)!

Combinatorial search

Exhaustive search. Iterate through all elements of a search space.

Applicability. Huge range of problems (include intractable ones).

Caveat. Search space is typically exponential in size \( \Rightarrow \) effectiveness may be limited to relatively small instances.

Backtracking. Systematic method for examining feasible solutions to a problem, by systematically pruning infeasible ones.

N-rooks problem

Q. How many ways are there to place \( N \) rooks on an \( N \times N \) board so that no rook can attack any other?

```
int[] a = { 2, 0, 1, 3, 6, 7, 4, 5 };
```

Representation. No two rooks in the same row or column \( \Rightarrow \) permutation.

Challenge. Enumerate all \( N! \) permutations of \( N \) integers 0 to \( N - 1 \).
Enumerating permutations

Recursive algorithm to enumerate all $N!$ permutations of $N$ elements.

- Start with permutation $a[0]$ to $a[N-1]$.
- For each value of $i$:
  - swap $a[i]$ into position 0
  - enumerate all $(N-1)!$ permutations of $a[1]$ to $a[N-1]$
  - clean up (swap $a[i]$ back to original position)

```
public class Rooks{
    private int N;
    private int[] a;  // bits (0 or 1)
    public Rooks(int N)   {
        this.N = N;
        a = new int[N];
        for (int i = 0; i < N; i++)
            a[i] = i;
        enumerate(0);
    }
    private void enumerate(int k){ /* see previous slide */
        if (k == N)   {
            process(); return;
        }
        for (int i = k; i < N; i++)   {
            exch(k, i);
            enumerate(k+1);
            exch(i, k);
        }
    }
    private void exch(int i, int j){  int t = a[i]; a[i] = a[j]; a[j] = t;  }
    public static void main(String[] args)   {
        int N = Integer.parseInt(args[0]);
        new Rooks(N);
    }
}
```

4-rooks search tree
**N-rooks problem: back-of-envelope running time estimate**

Slow way to compute $N!$.

Hypothesis. Running time is about $2 \left( \frac{N!}{8!} \right)$ seconds.

---

**N-queens problem**

Q. How many ways are there to place $N$ queens on an $N$-by-$N$ board so that no queen can attack any other?

Representation. No two queens in the same row or column $\Rightarrow$ permutation.

Additional constraint. No diagonal attack is possible.

Challenge. Enumerate (or even count) the solutions.

---

**4-queens search tree**

- diagonal conflict on partial solution: no point going deeper

- solutions

---

**4-queens search tree (pruned)**

- "backtrack" on diagonal conflicts

- solutions
**Backtracking**

**Backtracking paradigm.** Iterate through elements of search space.
- When there are several possible choices, make one choice and recur.
- If the choice is a dead end, backtrack to previous choice, and make next available choice.

**Benefit.** Identifying dead ends allows us to prune the search tree.

**Ex.** (backtracking for N-queens problem)
- Dead end: a diagonal conflict.
- Pruning: backtrack and try next column when diagonal conflict found.

**Applications.** Puzzles, combinatorial optimization, parsing, ...

---

**N-queens problem: effectiveness of backtracking**

Pruning the search tree leads to enormous time savings.

<table>
<thead>
<tr>
<th>N</th>
<th>Q(N)</th>
<th>N!</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>24</td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>120</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>720</td>
</tr>
<tr>
<td>7</td>
<td>40</td>
<td>5,040</td>
</tr>
<tr>
<td>8</td>
<td>92</td>
<td>40,320</td>
</tr>
<tr>
<td>9</td>
<td>352</td>
<td>362,880</td>
</tr>
<tr>
<td>10</td>
<td>724</td>
<td>3,628,800</td>
</tr>
<tr>
<td>11</td>
<td>2,680</td>
<td>39,916,800</td>
</tr>
<tr>
<td>12</td>
<td>14,200</td>
<td>479,001,600</td>
</tr>
<tr>
<td>13</td>
<td>73,712</td>
<td>6,227,020,800</td>
</tr>
<tr>
<td>14</td>
<td>365,596</td>
<td>87,178,291,200</td>
</tr>
</tbody>
</table>

---

**Hamilton path**

**Goal.** Find a simple path that visits every vertex exactly once.

**Remark.** Euler path easy, but Hamilton path is NP-complete.
Hamilton path: backtracking solution

Backtracking solution. To find Hamilton path starting at $v$:
- Add $v$ to current path.
- For each vertex $w$ adjacent to $v$:
  - find a simple path starting at $w$ using all remaining vertices
- Clean up: remove $v$ from current path.

Q. How to implement?
A. Add cleanup to DFS (!!)

That’s all, folks: keep searching!

The world’s longest path (Sendero de Chile): 9,700 km.  
(originally scheduled for completion in 2010; now delayed until 2038)