6.5 REDUCTIONS

- introduction
- designing algorithms
- establishing lower bounds
- classifying problems
- intractability

Overview: introduction to advanced topics

Main topics. [final two lectures]
- Reduction: relationship between two problems.
- Algorithm design: paradigms for solving problems.

Shifting gears.
- From individual problems to problem-solving models.
- From linear/quadratic to polynomial/exponential scale.
- From implementation details to conceptual frameworks.

Goals.
- Place algorithms and techniques we've studied in a larger context.
- Introduce you to important and essential ideas.
- Inspire you to learn more about algorithms!

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, element distinctness, closest pair, Euclidean MST, …</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 \( X \).

Cost of solving \( X \) = total cost of solving \( Y \) + cost of reduction.

Ex 1. [finding the median reduces to sorting]
To find the median of \( N \) items:
- Sort \( N \) items.
- Return item in the middle.

Cost of solving finding the median. \( N \log N + 1 \).

Reduction

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

Ex 2. [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. \( N \log N + N \).
Reduction

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

**Novice error.** Confusing $X$ reduces to $Y$ with $Y$ reduces to $X$.

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 $X$.

**More familiar reductions.**
- CPM reduces to topological sort.
- Arbitrage reduces to negative cycles.
- Bipartite matching reduces to maxflow.
- Seam carving reduces to shortest paths in a DAG.
- Burrows-Wheeler transform reduces to suffix sort.

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

3-collinear

**3-COLLINEAR.** Given $N$ distinct points in the plane, are there 3 (or more) that all lie on the same line?

**Brute force $N^3$.** For all triples of points $(p,q,r)$ check if they are collinear.
3-collinear reduces to sorting

Sorting-based algorithm. For each point $p$,
- Compute the slope that each other point $q$ makes with $p$.
- Sort the remaining $N-1$ points by slope.
- Collinear points are adjacent.

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

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.

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 in combinatorial optimization

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.

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. [Exceptions?]

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 \( Y \).
Element distinctness linear-time reduces to 2d closest pair

**Element distinctness.** Given $N$ elements, are any two equal?

**2d closest pair.** Given $N$ points in the plane, find the closest pair.

\[
\begin{align*}
590584 & -23439854 & 1251432 \\
-2861534 & 3988818 & -43434213 \\
333255 & 13546464 & 89885444 \\
& -43434213 & 11998833
\end{align*}
\]

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.

Some linear-time reductions in computational geometry

**3-SUM.** Given $N$ distinct integers, are there three that sum to 0?

**3-COLLINEAR.** Given $N$ distinct points in the plane, are there 3 (or more) that all lie on the same line?
Lower bound for 3-COLLINEAR

3-SUM. Given \( N \) distinct integers, are there three that sum to 0?

3-COLLINEAR. Given \( N \) distinct points in the plane, are there 3 (or more) that all lie on the same line?

**Proposition.** 3-SUM linear-time reduces to 3-COLLINEAR.

**Pf.** [next two slides]

Conjecture. Any algorithm for 3-SUM requires \( \Omega(N^{2-\epsilon}) \) steps.

Implication. No sub-quadratic algorithm for 3-COLLINEAR likely.

Complexity of 3-SUM

April 2014. Some recent evidence that the complexity might be \( N^{3/2} \).

3-SUM linear-time reduces to 3-COLLINEAR

**Proposition.** 3-SUM linear-time reduces to 3-COLLINEAR.

- 3-SUM instance: \( x_1, x_2, \ldots, x_N \).
- 3-COLLINEAR instance: \((x_1, x_1^3), (x_2, x_2^3), \ldots, (x_N, x_N^3)\).

**Lemma.** If \( a, b, \) and \( c \) are distinct, then \( a + b + c = 0 \) if and only if \((a, a^3), (b, b^3),\) and \((c, c^3)\) are collinear.

**Pf.** Three distinct points \((a, a^3), (b, b^3),\) and \((c, c^3)\) are collinear iff:

\[
0 = \begin{vmatrix} a & a^3 & 1 \\ b & b^3 & 1 \\ c & c^3 & 1 \end{vmatrix}
\]

\[= a(b^3 - c^3) - b(a^3 - c^3) + c(a^3 - b^3)\]

\[= (a - b)(b - c)(c - a)(a + b + c)\]
More geometric 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 Euclidean MST algorithm exists?


A2. [easy way] Linear-time reduction from element distinctness.

Classifying problems: summary

Desiderata. Problem with algorithm that matches lower bound.

Ex. Sorting and element distinctness 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)

assuming both take at least linear time
Integer arithmetic reductions

**Integer multiplication.** Given two $N$-bit integers, compute their product.

**Brute force.** $N^2$ bit operations.

\[
\begin{array}{cccccccc}
1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
\times & & & & & & & \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\hline
1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
\end{array}
\]

**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</td>
<td>$N^{1.585}$</td>
</tr>
<tr>
<td>1963</td>
<td>Toom–3, Toom–4</td>
<td>$N^{1.468}$, $N^{1.484}$</td>
</tr>
<tr>
<td>1966</td>
<td>Toom–Cook</td>
<td>$N^{1+\varepsilon}$</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.

<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?

Numerical linear algebra reductions

**Matrix multiplication.** Given two $N$-by-$N$ matrices, compute their product.

**Brute force.** $N^3$ flops.

\[
\begin{array}{cccc}
0.1 & 0.2 & 0.8 & 0.1 \\
0.5 & 0.3 & 0.9 & 0.6 \\
0.1 & 0.0 & 0.7 & 0.4 \\
0.0 & 0.3 & 0.3 & 0.1 \\
\end{array} \times
\begin{array}{cccc}
0.4 & 0.3 & 0.1 & 0.1 \\
0.2 & 0.2 & 0.0 & 0.6 \\
0.0 & 0.0 & 0.4 & 0.5 \\
0.8 & 0.4 & 0.1 & 0.9 \\
\end{array} =
\begin{array}{cccc}
0.16 & 0.11 & 0.34 & 0.62 \\
0.74 & 0.45 & 0.47 & 1.22 \\
0.36 & 0.19 & 0.33 & 0.72 \\
0.14 & 0.12 & 0.13 & 0.42 \\
\end{array}
\]

\[
0.5 \cdot 0.1 + 0.3 \cdot 0.0 + 0.9 \cdot 0.4 + 0.6 \cdot 0.1 = 0.47
\]
Numerical linear algebra reductions


<table>
<thead>
<tr>
<th>problem</th>
<th>linear algebra</th>
<th>order of growth</th>
</tr>
</thead>
<tbody>
<tr>
<td>matrix multiplication</td>
<td>$A \times B$</td>
<td>$O(N^3)$</td>
</tr>
<tr>
<td>matrix inversion</td>
<td>$A^{-1}$</td>
<td>$O(N^3)$</td>
</tr>
<tr>
<td>determinant</td>
<td>$LA$</td>
<td>$O(N^3)$</td>
</tr>
<tr>
<td>system of linear equations</td>
<td>$Ax = b$</td>
<td>$O(N^3)$</td>
</tr>
<tr>
<td>LU decomposition</td>
<td>$A = LU$</td>
<td>$O(N^3)$</td>
</tr>
<tr>
<td>least squares</td>
<td>$\min |Ax - bl|_2$</td>
<td>$O(N^3)$</td>
</tr>
</tbody>
</table>

numerical linear algebra problems with the same complexity as matrix multiplication

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>$N^{2.808}$</td>
</tr>
<tr>
<td>1978</td>
<td>Pan</td>
<td>$N^{2.796}$</td>
</tr>
<tr>
<td>1979</td>
<td>Bini</td>
<td>$N^{2.780}$</td>
</tr>
<tr>
<td>1981</td>
<td>Schönhage</td>
<td>$N^{2.522}$</td>
</tr>
<tr>
<td>1982</td>
<td>Romani</td>
<td>$N^{2.517}$</td>
</tr>
<tr>
<td>1982</td>
<td>Coppersmith–Winograd</td>
<td>$N^{2.496}$</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>$N^{2.337}$</td>
</tr>
<tr>
<td>2011</td>
<td>Williams</td>
<td>$N^{2.377}$</td>
</tr>
<tr>
<td>?</td>
<td>?</td>
<td>$N^{2 + c}$</td>
</tr>
</tbody>
</table>

number of floating-point operations to multiply two $N$-by-$N$ matrices

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.

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.
A core problem: satisfiability

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

Ex.

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

**3-SAT.** All equations of this form (with three variables per equation).

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

Satisfiability is conjectured to be intractable

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 (\( P \neq NP \)). 3-SAT is intractable (no poly-time algorithm).

Polynomial-time reductions

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

Establish intractability. If 3-SAT poly-time reduces to \( Y \), then \( Y \) is intractable.
(assuming 3-SAT is intractable)

Mentality.
- If I could solve \( Y \) in poly-time, then I could also solve 3-SAT in poly-time.
- 3-SAT is believed to be intractable.
- Therefore, so is \( Y \).

Integer linear programming

ILP. Given a system of linear inequalities, find an integral solution.

\[
\begin{align*}
3x_1 + 5x_2 + 2x_3 + x_4 + 4x_5 & \geq 10 \\
5x_1 + 2x_2 + 4x_4 + 1x_5 & \leq 7 \\
x_1 + x_3 + 2x_4 & \leq 2 \\
3x_1 + 4x_3 + 7x_4 & \leq 7 \\
x_1 + x_4 & \leq 1 \\
x_1 + x_3 + x_5 & \leq 1 \\
\text{all } x_i & = \{ 0, 1 \}
\end{align*}
\]

Context. Cornerstone problem in operations research.
Remark. Finding a real-valued solution is tractable (linear programming).
3-SAT poly-time reduces to ILP

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

\[
\neg x_1 \text{ or } x_2 \text{ or } x_3 = \text{true} \\
x_1 \text{ or } \neg x_2 \text{ or } x_3 = \text{true} \\
\neg x_1 \text{ or } \neg x_2 \text{ or } \neg x_3 = \text{true} \\
\neg x_1 \text{ or } \neg x_2 \text{ or } \neg x_3 \text{ or } x_4 = \text{true} \\
\neg x_2 \text{ or } x_3 \text{ or } x_4 = \text{true}
\]

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

\[
(1 - x_1) + x_2 + x_3 \geq 1 \\
x_1 + (1 - x_2) + x_3 \geq 1 \\
(1 - x_1) + (1 - x_2) + (1 - x_3) \geq 1 \\
(1 - x_1) + (1 - x_2) + x_4 \geq 1 \\
(1 - x_2) + x_3 + x_4 \geq 1
\]

solution to this ILP instance gives solution to original 3-SAT instance

Implications of poly-time reductions from 3-satisfiability

Establishing intractability through poly-time reduction is an important tool in guiding algorithm design efforts.

Q. How to convince yourself that a new problem is (probably) intractable?
A1. [hard way] Long futile search for an efficient algorithm (as for 3-SAT).
A2. [easy way] Reduction from 3-SAT.

Caveat. Intricate reductions are common.

More poly-time reductions from 3-satisfiability

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

Conjecture. 3-SAT is intractable.
Implication. All of these problems are intractable.

Search problems

Search problem. Problem where you can check a solution in poly-time.

Ex 1. 3-SAT.

\[
\neg x_1 \text{ or } x_2 \text{ or } x_3 = \text{true} \\
x_1 \text{ or } \neg x_2 \text{ or } x_3 = \text{true} \\
\neg x_1 \text{ or } \neg x_2 \text{ or } \neg x_3 = \text{true} \\
\neg x_1 \text{ or } \neg x_2 \text{ or } \neg x_3 \text{ or } x_4 = \text{true} \\
\neg x_2 \text{ or } x_3 \text{ or } x_4 = \text{true}
\]

instance I solution S

Ex 2. FACTOR. Given an N-bit integer x, find a nontrivial factor.

<table>
<thead>
<tr>
<th>instance I</th>
<th>solution S</th>
</tr>
</thead>
<tbody>
<tr>
<td>147573952589676412927</td>
<td>193707721</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>instance I</th>
<th>solution S</th>
</tr>
</thead>
<tbody>
<tr>
<td>x_1 x_2 x_3 x_4</td>
<td>T T F T</td>
</tr>
</tbody>
</table>
**P vs. NP**

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

*Importance.* What scientists and engineers can compute feasibly.

**NP.** Set of search problems (checkable in poly-time).

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

Fundamental question.

Consensus opinion. No.

---

**Cook-Levin theorem**

A problem is **NP-COMPLETE** if
- It is in NP.
- All problems in NP poly-time to reduce to it.

**Cook-Levin theorem.** 3-SAT is **NP-COMPLETE**.

*Corollary.* 3-SAT is tractable if and only if P = NP.

Two worlds.

---

**Implications of Cook-Levin theorem**

All of these problems (and many, many more) poly-time reduce to 3-SAT.

---

**Implications of Karp + Cook-Levin**

All of these problems are NP-complete; they are manifestations of the same really hard problem.
Birds-eye view: review

**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, element distinctness, ...</td>
</tr>
<tr>
<td>quadratic</td>
<td>$N^2$</td>
<td></td>
</tr>
<tr>
<td>exponential</td>
<td>$e^N$</td>
<td></td>
</tr>
</tbody>
</table>

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

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, Burrows-Wheeler transform, ...</td>
</tr>
<tr>
<td>linearithmic</td>
<td>$N \log N$</td>
<td>sorting, element distinctness, ...</td>
</tr>
<tr>
<td>quadratic</td>
<td>$N^2$</td>
<td>integer multiplication, division, square root, ...</td>
</tr>
<tr>
<td>MM(N)</td>
<td>possibly not</td>
<td>matrix multiplication, $Ax = b$, least square, determinant, ...</td>
</tr>
<tr>
<td>NP-complete</td>
<td>probably not $N^b$</td>
<td>3-SAT, IND-SET, ILP, ...</td>
</tr>
</tbody>
</table>

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

Complexity zoo

**Complexity class.** Set of problems sharing some computational property.

[Image of Complexity Zoo]

https://complexityzoo.uwaterloo.ca

**Bad news.** Lots of complexity classes (496 animals in zoo).

Summary

**Reductions are important in theory to:**
- Design algorithms.
- Establish lower bounds.
- 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, suffix arrays
  - MST, shortest paths, maxflow, linear programming
- Determine difficulty of your problem and choose the right tool.