"I can't find an efficient algorithm, I guess I'm just too dumb."
"I can’t find an efficient algorithm, because no such algorithm is possible!"
"I can't find an efficient algorithm, but neither can all these famous people."
Reductions

How do we show that a problem is easy?

Reduce each instance to one (or more) instances of a known easy problem.

\[ I_1 \in P_1 \quad R(I_1) = I_2 \in P_2 \]

To solve \( I_1 \) in \( P_2 \):

1. Apply \( R \) to turn \( I_1 \) into \( I_2 \in P_2 \)
2. Apply algorithm for \( P_2 \) to \( I_2 \).

Cost = cost of applying \( R \) plus cost of applying \( P_2 \) algorithm.
Examples

Reduction to some form of matrix multiplication:

Transitive closure

Context-free language recognition

Reduction to linear programming

Reduction to network flow

etc.

Cost of reduction?

linear time, quadratic time, ...
Positive use of reduction:

\[ ? \Rightarrow \text{easy} \]

Reduce a problem of unknown complexity to an easy problem

"Negative" use of reduction:

How do we show that a problem of unknown complexity is hard?

Reduce a hard problem to it

\[ \text{hard} \Rightarrow ? \]

If the questionable problem were easy, so would be the hard problem.
Reductions in both directions show computational equivalence (up to the cost of the reduction)

\[ P_1 \Leftrightarrow P_2 \]

both are easy or both are hard

Transitivity of reductions

\[ P_1 \Rightarrow P_2 \Rightarrow P_3 \]

\[ R_1 \quad R_2 \]

Gives a reduction from \( P_1 \) to \( P_3 \)

Cost is cost of \( R_2 \circ (R_1(\cdot)) \)

both p-time, overall p-time

linear linear
\[ R_1 \quad R_2 \]
\[ n \quad an \quad bn \]
\[ an \quad (ab)n \]
\[ n \quad an^2 \quad bn^2 \]
\[ an^2 \quad b(a^2)^2 = ba^2 n^4 \]
\[ \frac{k}{n} \quad bn^l \]
\[ b(an^l)^l = b a^l n^{kl} \]
Satisfiability: Is a Boolean (logical) function true for some choice of variable assignments?

\((x \lor y) \land (\bar{x} \lor \bar{y})\)  \(\text{sat}: x=1, y=0\)

\(\land\) and
\(\lor\) or
\(-\) not

\(x\) variable
\(x, \bar{x}\) literal

\((x \lor y \lor z)\) clause: disjunction ("or") of literals
\((x \lor y \lor z) \land (\bar{x} \lor \bar{y} \lor \bar{z})\) conjunctive normal form:
conjunct ("and") of clauses

\(x \lor \bar{x}\) tautology: true for all choices of variables

\(F\) is sat iff \(F\) is not a tautology:
can be falsified
Reduction of CNF sat to 3-CNF sat
(at most 3 literals/clause)

\[(x \lor y \lor z \lor w \lor u \lor v) \Rightarrow \]
\[(x \lor y \lor a) \land (\bar{a} \lor z \lor b) \land (b \lor w \lor c) \land (\bar{c} \lor u \lor v)\]

Needs \(k-3\) extra vars per clause of length \(k\).
Graph coloring reducible to sat,

and vice-versa \((\text{P-time reductions})\)

Must phrase graph coloring as a yes-no question: can graph \(G\) be colored with \(k\) colors?

\(G: n\) vertices, \(m\) edges

\(F: nk\) variables \(x_{ij}\), one per vertex per color

\(x_{ij}\) true iff vertex \(i\) colored color \(j\)

Clauses:

Each vertex colored
\[
(x_{i1} \lor x_{i2} \lor \ldots \lor x_{ik}) \quad i \in V, \quad 1 \leq i \leq n
\]

No vertex colored twice
\[
(\bar{x}_{ij} \lor \bar{x}_{il}) \quad i \in V, \quad j \neq l \text{ colors} \quad 1 \leq j, l \leq k
\]

No adjacent vertices the same color
\[
(\bar{x}_{i1} \lor \bar{x}_{j1}) \quad (i, j) \in E, \quad l \text{ a color} \quad 1 \leq l \leq k
\]

\# literals = \(nk + 2n(k/2) + 2 mk\)
Vice-versa: (3-sat)

Reduction to 3-coloring

Vertices: $x, \bar{x}$, true, false, red, 5 per clause

$x, \bar{x}$ colored
true, false

Clause $x \lor \bar{y} \lor \bar{z}$

Colorable iff formula satisfiable

"gadget" for each clause
satisfiable (SAT) \implies Clique

Given a graph, are there \( k \) pairwise adjacent vertices?

One vertex per literal occurrence,

two vertices in different clauses joined by an edge if compatible (not \( x, \overline{x} \))

\( k = \# \) clauses

\[
(x \lor y \lor z) \quad (\overline{x} \lor y \lor z)
\]

\[
(x \lor y \lor \overline{w}) \quad (x \lor y \lor \overline{w})
\]

\[
(x \lor y \lor \overline{w} \lor u)
\]
Clique $\Rightarrow$ Sat

$x_{ij} \in \{0, 1\} \quad 1 \leq j < k$

$x_{ij}$ true = vertex $i$ is $j^{th}$ in clique

$i, b \in V \text{ not adj.}$

$(\bar{x}_{ij} \lor \bar{x}_{ij'}) \forall j, j'$

$(\bar{x}_{ij} \lor \bar{x}_{ij'}) \quad i \neq i', \forall j$

$(x_{ij} \lor x_{ij'} \lor \ldots \lor x_{ij''}) \forall j$
Clique $\Leftrightarrow$ Independent set

Are there $k$ pairwise nonadjacent vertices?

Complement graph

Clique $\Leftrightarrow$ Vertex cover

Are there $k$ vertices "covering" all edges

$S$ a vertex cover in $G$ iff

$V-S$ is an independent set in $G$ iff

$V-S$ is a clique in $\overline{G}$
P = problems solvable in p-time

NP = yes-no problems s.t. if answer is “yes”, can be verified in p-time given a (p-length) “proof” (hint).

p-time on a Turing machine
or random-access machine