CS 473: Fundamental Algorithms, Spring 2013

Reductions and NP

Lecture 21
April 11, 2013

Part I

Reductions Continued

Polynomial Time Reduction

Karp reduction

A **polynomial time reduction** from a *decision* problem $\mathbf{X}$ to a *decision* problem $\mathbf{Y}$ is an *algorithm* $\mathcal{A}$ that has the following properties:

1. given an instance $\mathbf{I_X}$ of $\mathbf{X}$, $\mathcal{A}$ produces an instance $\mathbf{I_Y}$ of $\mathbf{Y}$
2. $\mathcal{A}$ runs in time polynomial in $|\mathbf{I_X}|$. This implies that $|\mathbf{I_Y}|$ (size of $\mathbf{I_Y}$) is polynomial in $|\mathbf{I_X}|$
3. Answer to $\mathbf{I_X}$ YES *iff* answer to $\mathbf{I_Y}$ is YES.

Notation: $\mathbf{X} \leq_P \mathbf{Y}$ if $\mathbf{X}$ reduces to $\mathbf{Y}$

Proposition

If $\mathbf{X} \leq_P \mathbf{Y}$ then a polynomial time algorithm for $\mathbf{Y}$ implies a polynomial time algorithm for $\mathbf{X}$.

Such a reduction is called a **Karp reduction**. Most reductions we will need are Karp reductions.

A More General Reduction

Turing Reduction

Definition (Turing reduction.)

Problem $\mathbf{X}$ polynomial time reduces to $\mathbf{Y}$ if there is an algorithm $\mathcal{A}$ for $\mathbf{X}$ that has the following properties:

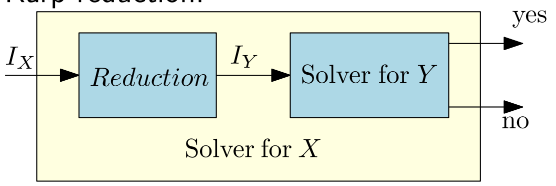
1. on any given instance $\mathbf{I_X}$ of $\mathbf{X}$, $\mathcal{A}$ uses polynomial in $|\mathbf{I_X}|$ "steps"
2. a step is either a standard computation step, or
3. a sub-routine call to an algorithm that solves $\mathbf{Y}$.

This is a **Turing reduction**.

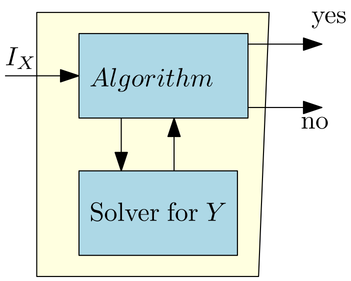
Note: In making sub-routine call to algorithm to solve $\mathbf{Y}$, $\mathcal{A}$ can only ask questions of size polynomial in $|\mathbf{I_X}|$. Why?

Comparing reductions

1. Karp reduction:



2. Turing reduction:



Turing reduction

1. Algorithm to solve **X** can call solver for **Y** many times.
2. Conceptually, every call to the solver of **Y** takes constant time.

Example of Turing Reduction

Problem (Independent set in circular arcs graph.)

Input: *Collection of arcs on a circle.*
Goal: *Compute the maximum number of non-overlapping arcs.*

Reduced to the following problem:?

Problem (Independent set of intervals.)

Input: *Collection of intervals on the line.*
Goal: *Compute the maximum number of non-overlapping intervals.*

How? Used algorithm for interval problem multiple times.

Turing vs Karp Reductions

1. Turing reductions more general than Karp reductions.
2. Turing reduction useful in obtaining algorithms via reductions.
3. Karp reduction is simpler and easier to use to prove hardness of problems.
4. Perhaps surprisingly, Karp reductions, although limited, suffice for most known **NP-Complete**ness proofs.
5. Karp reductions allow us to distinguish between **NP** and **co-NP** (more on this later).

Propositional Formulas

Definition

Consider a set of boolean variables $x_1, x_2, \ldots x_n$.

1. A **literal** is either a boolean variable x_i or its negation $\neg x_i$.
2. A **clause** is a disjunction of literals.
   For example, $x_1 \vee x_2 \vee \neg x_4$ is a clause.
3. A **formula in conjunctive normal form** (CNF) is propositional formula which is a conjunction of clauses
   1. $(x_1 \vee x_2 \vee \neg x_4) \wedge (x_2 \vee \neg x_3) \wedge x_5$ is a CNF formula.
4. A formula φ is a 3CNF:
   A CNF formula such that every clause has **exactly** 3 literals.
   1. $(x_1 \vee x_2 \vee \neg x_4) \wedge (x_2 \vee \neg x_3 \vee x_1)$ is a 3CNF formula, but $(x_1 \vee x_2 \vee \neg x_4) \wedge (x_2 \vee \neg x_3) \wedge x_5$ is not.

Satisfiability

Problem: SAT

Instance: A CNF formula φ. **Question:** Is there a truth assignment to the variable of φ such that φ evaluates to true?

Problem: 3SAT

Instance: A 3CNF formula φ. **Question:** Is there a truth assignment to the variable of φ such that φ evaluates to true?

Satisfiability

SAT

Given a CNF formula φ, is there a truth assignment to variables such that φ evaluates to true?

Example

1. $(x_1 \vee x_2 \vee \neg x_4) \wedge (x_2 \vee \neg x_3) \wedge x_5$ is satisfiable; take $x_1, x_2, \ldots x_5$ to be all true
2. $(x_1 \vee \neg x_2) \wedge (\neg x_1 \vee x_2) \wedge (\neg x_1 \vee \neg x_2) \wedge (x_1 \vee x_2)$ is not satisfiable.

3SAT

Given a 3CNF formula φ, is there a truth assignment to variables such that φ evaluates to true?

(More on **2SAT** in a bit...)

Importance of SAT and 3SAT

1. **SAT** and **3SAT** are basic constraint satisfaction problems.
2. Many different problems can reduced to them because of the simple yet powerful expressively of logical constraints.
3. Arise naturally in many applications involving hardware and software verification and correctness.
4. As we will see, it is a fundamental problem in theory of **NP-Complete**ness.

SAT $\leq_P$ 3SAT

How SAT is different from 3SAT?

In **SAT** clauses might have arbitrary length: $1, 2, 3, \ldots$ variables:

$$\Big(x \vee y \vee z \vee w \vee u\Big) \wedge \Big(\neg x \vee \neg y \vee \neg z \vee w \vee u\Big) \wedge \Big(\neg x\Big)$$

In **3SAT** every clause must have **exactly 3** different literals.

To reduce from an instance of **SAT** to an instance of **3SAT**, we must make all clauses to have exactly **3** variables...

Basic idea

1. Pad short clauses so they have **3** literals.
2. Break long clauses into shorter clauses.
3. Repeat the above till we have a 3CNF.

3SAT $\leq_P$ SAT

1. **3SAT** $\leq_P$ **SAT**.
2. Because...
   A **3SAT** instance is also an instance of **SAT**.

SAT $\leq_P$ 3SAT

Claim

SAT $\leq_P$ **3SAT**.

Given φ a **SAT** formula we create a **3SAT** formula φ' such that

1. φ is satisfiable iff φ' is satisfiable.
2. φ' can be constructed from φ in time polynomial in $|\varphi|$.

Idea: if a clause of φ is not of length $\mathbf{3}$, replace it with several clauses of length exactly $\mathbf{3}$.

SAT $\leq_P$ 3SAT

A clause with a single literal

Reduction Ideas

Challenge: Some of the clauses in φ may have less or more than $\mathbf{3}$ literals. For each clause with $< \mathbf{3}$ or $> \mathbf{3}$ literals, we will construct a set of logically equivalent clauses.

1. Case clause with one literal: Let $\mathbf{c}$ be a clause with a single literal (i.e., $\mathbf{c} = \ell$). Let $\mathbf{u}, \mathbf{v}$ be new variables. Consider

$$\mathbf{c}' = \Big(\ell \vee \mathbf{u} \vee \mathbf{v}\Big) \wedge \Big(\ell \vee \mathbf{u} \vee \neg\mathbf{v}\Big) \wedge \Big(\ell \vee \neg\mathbf{u} \vee \mathbf{v}\Big) \wedge \Big(\ell \vee \neg\mathbf{u} \vee \neg\mathbf{v}\Big).$$

   Observe that $\mathbf{c}'$ is satisfiable iff $\mathbf{c}$ is satisfiable

SAT $\leq_P$ 3SAT

A clause with two literals

Reduction Ideas: 2 and more literals

1. Case clause with 2 literals: Let $\mathbf{c} = \ell_1 \vee \ell_2$. Let $\mathbf{u}$ be a new variable. Consider

$$\mathbf{c}' = \Big(\ell_1 \vee \ell_2 \vee \mathbf{u}\Big) \wedge \Big(\ell_1 \vee \ell_2 \vee \neg\mathbf{u}\Big).$$

   Again $\mathbf{c}$ is satisfiable iff $\mathbf{c}'$ is satisfiable

Breaking a clause

Lemma

For any boolean formulas $\mathbf{X}$ *and* $\mathbf{Y}$ *and* $\mathbf{z}$ *a new boolean variable. Then*

$$\mathbf{X} \vee \mathbf{Y} \text{ is satisfiable}$$

if and only if, $\mathbf{z}$ *can be assigned a value such that*

$$\left(\mathbf{X} \vee \mathbf{z}\right) \wedge \left(\mathbf{Y} \vee \neg \mathbf{z}\right) \text{ is satisfiable}$$

(with the same assignment to the variables appearing in $\mathbf{X}$ *and* $\mathbf{Y}$*).*

SAT $\leq_P$ 3SAT (contd)

Clauses with more than 3 literals

Let $\mathbf{c} = \ell_1 \vee \cdots \vee \ell_k$. Let $\mathbf{u}_1, \ldots \mathbf{u}_{k-3}$ be new variables. Consider

$$\mathbf{c}' = \left(\ell_1 \vee \ell_2 \vee \mathbf{u}_1\right) \wedge \left(\ell_3 \vee \neg \mathbf{u}_1 \vee \mathbf{u}_2\right) \wedge \left(\ell_4 \vee \neg \mathbf{u}_2 \vee \mathbf{u}_3\right) \wedge \cdots \wedge \left(\ell_{k-2} \vee \neg \mathbf{u}_{k-4} \vee \mathbf{u}_{k-3}\right) \wedge \left(\ell_{k-1} \vee \ell_k \vee \neg \mathbf{u}_{k-3}\right).$$

Claim

$\mathbf{c}$ *is satisfiable iff* $\mathbf{c}'$ *is satisfiable.*

Another way to see it — reduce size of clause by one:

$$\mathbf{c}' = \left(\ell_1 \vee \ell_2 \ldots \vee \ell_{k-2} \vee \mathbf{u}_{k-3}\right) \wedge \left(\ell_{k-1} \vee \ell_k \vee \neg \mathbf{u}_{k-3}\right).$$

An Example

Example

$$\varphi = \left(\neg \mathbf{x}_1 \vee \neg \mathbf{x}_4\right) \wedge \left(\mathbf{x}_1 \vee \neg \mathbf{x}_2 \vee \neg \mathbf{x}_3\right) \wedge \left(\neg \mathbf{x}_2 \vee \neg \mathbf{x}_3 \vee \mathbf{x}_4 \vee \mathbf{x}_1\right) \wedge \left(\mathbf{x}_1\right).$$

Equivalent form:

$$\begin{aligned}\psi = & (\neg \mathbf{x}_1 \vee \neg \mathbf{x}_4 \vee \mathbf{z}) \wedge (\neg \mathbf{x}_1 \vee \neg \mathbf{x}_4 \vee \neg \mathbf{z}) \\ & \wedge (\mathbf{x}_1 \vee \neg \mathbf{x}_2 \vee \neg \mathbf{x}_3) \\ & \wedge (\neg \mathbf{x}_2 \vee \neg \mathbf{x}_3 \vee \mathbf{y}_1) \wedge (\mathbf{x}_4 \vee \mathbf{x}_1 \vee \neg \mathbf{y}_1) \\ & \wedge (\mathbf{x}_1 \vee \mathbf{u} \vee \mathbf{v}) \wedge (\mathbf{x}_1 \vee \mathbf{u} \vee \neg \mathbf{v}) \\ & \wedge (\mathbf{x}_1 \vee \neg \mathbf{u} \vee \mathbf{v}) \wedge (\mathbf{x}_1 \vee \neg \mathbf{u} \vee \neg \mathbf{v}).\end{aligned}$$

Overall Reduction Algorithm

Reduction from SAT to 3SAT

```
ReduceSATTo3SAT(φ):
    // φ: CNF formula.
    for each clause c of φ do
        if c does not have exactly 3 literals then
            construct c' as before
        else
            c' = c
    ψ is conjunction of all c' constructed in loop
    return Solver3SAT(ψ)
```

Correctness (informal)

φ is satisfiable iff ψ is satisfiable because for each clause $\mathbf{c}$, the new 3CNF formula $\mathbf{c}'$ is logically equivalent to $\mathbf{c}$.

What about 2SAT?

2SAT can be solved in polynomial time! (specifically, linear time!)

No known polynomial time reduction from **SAT** (or **3SAT**) to **2SAT**. If there was, then **SAT** and **3SAT** would be solvable in polynomial time.

Why the reduction from 3SAT to 2SAT fails?

Consider a clause $(\mathbf{x} \vee \mathbf{y} \vee \mathbf{z})$. We need to reduce it to a collection of $\mathbf{2}\mathrm{CNF}$ clauses. Introduce a face variable α, and rewrite this as

$$(\mathbf{x} \vee \mathbf{y} \vee \alpha) \wedge (\neg\alpha \vee \mathbf{z}) \qquad \text{(bad! clause with 3 vars)}$$

or $$(\mathbf{x} \vee \alpha) \wedge (\neg\alpha \vee \mathbf{y} \vee \mathbf{z}) \qquad \text{(bad! clause with 3 vars).}$$

(In animal farm language: **2SAT** good, **3SAT** bad.)

What about 2SAT?

A challenging exercise: Given a **2SAT** formula show to compute its satisfying assignment...
(Hint: Create a graph with two vertices for each variable (for a variable $\mathbf{x}$ there would be two vertices with labels $\mathbf{x} = \mathbf{0}$ and $\mathbf{x} = \mathbf{1}$). For ever $\mathbf{2}\mathrm{CNF}$ clause add two directed edges in the graph. The edges are implication edges: They state that if you decide to assign a certain value to a variable, then you must assign a certain value to some other variable.
Now compute the strong connected components in this graph, and continue from there...)

Independent Set

Problem: Independent Set

Instance: A graph G, integer $\mathbf{k}$.
Question: Is there an independent set in G of size $\mathbf{k}$?

3SAT $\leq_P$ Independent Set

The reduction 3SAT $\leq_P$ Independent Set

Input: Given a $3\mathrm{CNF}$ formula φ
Goal: Construct a graph $\mathbf{G}_\varphi$ and number $\mathbf{k}$ such that $\mathbf{G}_\varphi$ has an independent set of size $\mathbf{k}$ if and only if φ is satisfiable.
$\mathbf{G}_\varphi$ should be constructable in time polynomial in size of φ

Importance of reduction: Although **3SAT** is much more expressive, it can be reduced to a seemingly specialized Independent Set problem.

Notice: We handle only $3\mathrm{CNF}$ formulas – reduction would not work for other kinds of boolean formulas.

Interpreting 3SAT

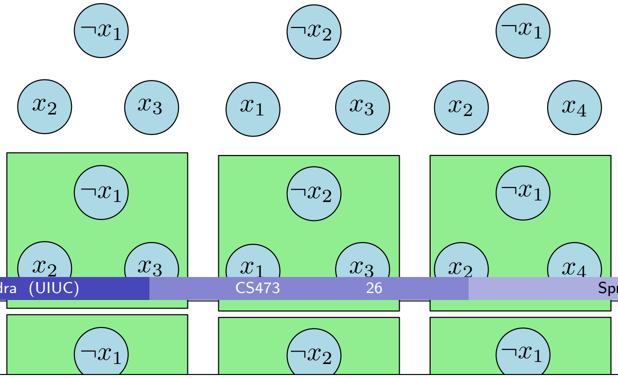
There are two ways to think about **3SAT**

1. Find a way to assign 0/1 (false/true) to the variables such that the formula evaluates to true, that is each clause evaluates to true.
2. Pick a literal from each clause and find a truth assignment to make all of them true. You will fail if two of the literals you pick are in conflict, i.e., you pick $\mathbf{x_i}$ and $\neg \mathbf{x_i}$

We will take the second view of **3SAT** to construct the reduction.

The Reduction

1. $\mathbf{G}_\varphi$ will have one vertex for each literal in a clause
2. Connect the 3 literals in a clause to form a triangle; the independent set will pick at most one vertex from each clause, which will correspond to the literal to be set to true
3. Connect 2 vertices if they label complementary literals; this ensures that the literals corresponding to the independent set do not have a conflict
4. Take **k** to be the number of clauses



Correctness

Proposition

φ is satisfiable iff $\mathbf{G}_\varphi$ has an independent set of size $\mathbf{k}$ (= number of clauses in φ).

Proof.

$\Rightarrow$ Let **a** be the truth assignment satisfying φ

1. Pick one of the vertices, corresponding to true literals under **a**, from each triangle. This is an independent set of the appropriate size ☐

Correctness (contd)

Proposition

φ is satisfiable iff $\mathbf{G}_\varphi$ has an independent set of size $\mathbf{k}$ (= number of clauses in φ).

Proof.

$\Leftarrow$ Let **S** be an independent set of size **k**

1. **S** must contain exactly one vertex from each clause
2. **S** cannot contain vertices labeled by conflicting clauses
3. Thus, it is possible to obtain a truth assignment that makes in the literals in **S** true; such an assignment satisfies one literal in every clause ☐

Transitivity of Reductions

Lemma

$\mathbf{X} \leq_P \mathbf{Y}$ *and* $\mathbf{Y} \leq_P \mathbf{Z}$ *implies that* $\mathbf{X} \leq_P \mathbf{Z}$.

Note: $\mathbf{X} \leq_P \mathbf{Y}$ does not imply that $\mathbf{Y} \leq_P \mathbf{X}$ and hence it is very important to know the FROM and TO in a reduction.

To prove $\mathbf{X} \leq_P \mathbf{Y}$ you need to show a reduction FROM $\mathbf{X}$ TO $\mathbf{Y}$
In other words show that an algorithm for $\mathbf{Y}$ implies an algorithm for $\mathbf{X}$.

Part II

Definition of NP

Recap . . .

Problems

1. **Independent Set**
2. **Vertex Cover**
3. **Set Cover**
4. **SAT**
5. **3SAT**

Relationship

3SAT $\leq_P$ **Independent Set** $\overset{\leq_P}{\geq_P}$ **Vertex Cover** $\leq_P$ **Set Cover**
3SAT $\leq_P$ **SAT** $\leq_P$ **3SAT**

Problems and Algorithms: Formal Approach

Decision Problems

1. Problem Instance: Binary string $\mathbf{s}$, with size $|\mathbf{s}|$
2. Problem: A set $\mathbf{X}$ of strings on which the answer should be "yes"; we call these YES instances of $\mathbf{X}$. Strings not in $\mathbf{X}$ are NO instances of $\mathbf{X}$.

Definition

1. $\mathbf{A}$ is an algorithm for problem $\mathbf{X}$ if $\mathbf{A(s)} =$ "yes" iff $\mathbf{s} \in \mathbf{X}$.
2. $\mathbf{A}$ is said to have a polynomial running time if there is a polynomial $\mathbf{p(\cdot)}$ such that for every string $\mathbf{s}$, $\mathbf{A(s)}$ terminates in at most $\mathbf{O(p(|s|))}$ steps.

Polynomial Time

Definition

Polynomial time (denoted by $\mathbf{P}$) is the class of all (decision) problems that have an algorithm that solves it in polynomial time.

Example

Problems in $\mathbf{P}$ include

1. Is there a shortest path from $\mathbf{s}$ to $\mathbf{t}$ of length $\leq \mathbf{k}$ in $\mathbf{G}$?
2. Is there a flow of value $\geq \mathbf{k}$ in network $\mathbf{G}$?
3. Is there an assignment to variables to satisfy given linear constraints?

Efficiency Hypothesis

A problem $\mathbf{X}$ *has an efficient algorithm iff* $\mathbf{X} \in \mathbf{P}$, *that is* $\mathbf{X}$ *has a polynomial time algorithm.*

Justifications:

1. Robustness of definition to variations in machines.
2. A sound theoretical definition.
3. Most known polynomial time algorithms for "natural" problems have small polynomial running times.

Problems with no known polynomial time algorithms

Problems

1. **Independent Set**
2. **Vertex Cover**
3. **Set Cover**
4. **SAT**
5. **3SAT**

There are of course undecidable problems (no algorithm at all!) but many problems that we want to solve are of similar flavor to the above.

Question: What is common to above problems?

Efficient Checkability

Above problems share the following feature:

Checkability

For any YES instance $\mathbf{I_X}$ *of* $\mathbf{X}$ *there is a proof/certificate/solution that is of length poly(*$|\mathbf{I_X}|$*) such that given a proof one can efficiently check that* $\mathbf{I_X}$ *is indeed a YES instance.*

Examples:

1. **SAT** formula φ: proof is a satisfying assignment.
2. **Independent Set** in graph $\mathbf{G}$ and $\mathbf{k}$: a subset $\mathbf{S}$ of vertices.

Certifiers

Definition

An algorithm $\mathbf{C}(\cdot, \cdot)$ is a **certifier** for problem $\mathbf{X}$ if for every $\mathbf{s} \in \mathbf{X}$ there is some string $\mathbf{t}$ such that $\mathbf{C}(\mathbf{s}, \mathbf{t}) =$ "yes", and conversely, if for some $\mathbf{s}$ and $\mathbf{t}$, $\mathbf{C}(\mathbf{s}, \mathbf{t}) =$ "yes" then $\mathbf{s} \in \mathbf{X}$.
The string $\mathbf{t}$ is called a certificate or proof for $\mathbf{s}$.

Definition (Efficient Certifier.)

A certifier $\mathbf{C}$ is an **efficient certifier** for problem $\mathbf{X}$ if there is a polynomial $\mathbf{p}(\cdot)$ such that for every string $\mathbf{s}$, we have that

- ⋆ $\mathbf{s} \in \mathbf{X}$ if and only if
- ⋆ there is a string $\mathbf{t}$:
  1. $|\mathbf{t}| \leq \mathbf{p}(|\mathbf{s}|)$,
  2. $\mathbf{C}(\mathbf{s}, \mathbf{t}) =$ "yes",
  3. and $\mathbf{C}$ runs in polynomial time.

Example: Independent Set

1. Problem: Does $\mathbf{G} = (\mathbf{V}, \mathbf{E})$ have an independent set of size $\geq \mathbf{k}$?
   1. Certificate: Set $\mathbf{S} \subseteq \mathbf{V}$.
   2. Certifier: Check $|\mathbf{S}| \geq \mathbf{k}$ and no pair of vertices in $\mathbf{S}$ is connected by an edge.

Example: Vertex Cover

1. Problem: Does $\mathbf{G}$ have a vertex cover of size $\leq \mathbf{k}$?
   1. Certificate: $\mathbf{S} \subseteq \mathbf{V}$.
   2. Certifier: Check $|\mathbf{S}| \leq \mathbf{k}$ and that for every edge at least one endpoint is in $\mathbf{S}$.

Example: SAT

1. Problem: Does formula φ have a satisfying truth assignment?
   1. Certificate: Assignment $\mathbf{a}$ of $\mathbf{0}/\mathbf{1}$ values to each variable.
   2. Certifier: Check each clause under $\mathbf{a}$ and say "yes" if all clauses are true.

Example:Composites

Problem: Composite

Instance: A number $\mathbf{s}$. **Question:** Is the number $\mathbf{s}$ a composite?

1. Problem: **Composite**.
   1. Certificate: A factor $\mathbf{t} \leq \mathbf{s}$ such that $\mathbf{t} \neq \mathbf{1}$ and $\mathbf{t} \neq \mathbf{s}$.
   2. Certifier: Check that $\mathbf{t}$ divides $\mathbf{s}$.

Nondeterministic Polynomial Time

Definition

Nondeterministic Polynomial Time (denoted by **NP**) is the class of all problems that have efficient certifiers.

Example

Independent Set, **Vertex Cover**, **Set Cover**, **SAT**, **3SAT**, and **Composite** are all examples of problems in **NP**.

Why is it called...

Nondeterministic Polynomial Time

A certifier is an algorithm $\mathbf{C}(\mathbf{I}, \mathbf{c})$ with two inputs:

1. $\mathbf{I}$: instance.
2. $\mathbf{c}$: proof/certificate that the instance is indeed a YES instance of the given problem.

One can think about $\mathbf{C}$ as an algorithm for the original problem, if:

1. Given $\mathbf{I}$, the algorithm guess (non-deterministically, and who knows how) the certificate $\mathbf{c}$.
2. The algorithm now verifies the certificate $\mathbf{c}$ for the instance $\mathbf{I}$.

Usually **NP** is described using Turing machines (gag).

Asymmetry in Definition of NP

Note that only YES instances have a short proof/certificate. NO instances need not have a short certificate.

Example

SAT formula φ. No easy way to prove that φ is NOT satisfiable!

More on this and **co-NP** later on.

P versus NP

Proposition

$\mathbf{P} \subseteq \mathbf{NP}$.

For a problem in **P** no need for a certificate!

Proof.

Consider problem $\mathbf{X} \in \mathbf{P}$ with algorithm $\mathbf{A}$. Need to demonstrate that $\mathbf{X}$ has an efficient certifier:

1. Certifier $\mathbf{C}$ on input $\mathbf{s}, \mathbf{t}$, runs $\mathbf{A}(\mathbf{s})$ and returns the answer.
2. $\mathbf{C}$ runs in polynomial time.
3. If $\mathbf{s} \in \mathbf{X}$, then for every $\mathbf{t}$, $\mathbf{C}(\mathbf{s}, \mathbf{t}) =$ "yes".
4. If $\mathbf{s} \notin \mathbf{X}$, then for every $\mathbf{t}$, $\mathbf{C}(\mathbf{s}, \mathbf{t}) =$ "no". □

Exponential Time

Definition

Exponential Time (denoted **EXP**) is the collection of all problems that have an algorithm which on input $\mathbf{s}$ runs in exponential time, i.e., $\mathbf{O}(2^{\mathrm{poly}(|\mathbf{s}|)})$.

Example: $\mathbf{O}(2^{\mathbf{n}})$, $\mathbf{O}(2^{\mathbf{n} \log \mathbf{n}})$, $\mathbf{O}(2^{\mathbf{n}^3})$, ...

NP versus EXP

Proposition

$\mathbf{NP} \subseteq \mathbf{EXP}$.

Proof.

Let $\mathbf{X} \in \mathbf{NP}$ with certifier $\mathbf{C}$. Need to design an exponential time algorithm for $\mathbf{X}$.

1. For every $\mathbf{t}$, with $|\mathbf{t}| \leq \mathbf{p}(|\mathbf{s}|)$ run $\mathbf{C}(\mathbf{s}, \mathbf{t})$; answer "yes" if any one of these calls returns "yes".
2. The above algorithm correctly solves $\mathbf{X}$ (exercise).
3. Algorithm runs in $\mathbf{O}(\mathbf{q}(|\mathbf{s}| + |\mathbf{p}(\mathbf{s})|)2^{\mathbf{p}(|\mathbf{s}|)})$, where $\mathbf{q}$ is the running time of $\mathbf{C}$. □

Examples

1. **SAT**: try all possible truth assignment to variables.
2. **Independent Set**: try all possible subsets of vertices.
3. **Vertex Cover**: try all possible subsets of vertices.

Is NP efficiently solvable?

We know $\mathbf{P} \subseteq \mathbf{NP} \subseteq \mathbf{EXP}$.

Big Question

Is there are problem in **NP** that does not belong to **P**? Is $\mathbf{P} = \mathbf{NP}$?

If P = NP . . .

Or: If pigs could fly then life would be sweet.

1. Many important optimization problems can be solved efficiently.
2. The RSA cryptosystem can be broken.
3. No security on the web.
4. No e-commerce . . .
5. Creativity can be automated! Proofs for mathematical statement can be found by computers automatically (if short ones exist).

P versus NP

Status

Relationship between **P** and **NP** remains one of the most important open problems in mathematics/computer science.

Consensus: Most people feel/believe $\mathbf{P} \neq \mathbf{NP}$.

Resolving **P** versus **NP** is a Clay Millennium Prize Problem. You can win a million dollars in addition to a Turing award and major fame!

Part III

Not for lecture: Converting any boolean formula into CNF

The dark art of formula conversion into CNF

Consider an arbitrary boolean formula ϕ defined over $\mathbf{k}$ variables. To keep the discussion concrete, consider the formula $\phi \equiv \mathsf{x_k} = \mathsf{x_i} \wedge \mathsf{x_j}$. We would like to convert this formula into an equivalent CNF formula.

Formula conversion into CNF

Step 1

Build a truth table for the boolean formula.

$\mathsf{x_k}$	$\mathsf{x_i}$	$\mathsf{x_j}$	value of $\mathsf{x_k} = \mathsf{x_i} \wedge \mathsf{x_j}$
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

Formula conversion into CNF

Step 1.5 - understand what a single CNF clause represents

Given an assignment, say, $\mathsf{x_k} = \mathbf{1}$, $\mathbf{k_i} = \mathbf{1}$ and $\mathbf{k_j} = \mathbf{0}$, consider the CNF clause $\mathsf{x_k} \vee \mathsf{x_i} \vee \overline{\mathsf{x_j}}$ (you negate a variable if it is assigned zero). Its truth table is

$\mathsf{x_k}$	$\mathsf{x_i}$	$\mathsf{x_j}$	$\mathsf{x_k} \vee \mathsf{x_i} \vee \overline{\mathsf{x_j}}$
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	1

Observe that a single clause assigns zero to one row, and one everywhere else. An conjunction of several such clauses, as such, would result in a formula that is 0 in all the rows that corresponds to these clauses, and one everywhere else.

Formula conversion into CNF

Step 2

Write down the CNF clause for every row in the table that is zero.

$\mathsf{x_k}$	$\mathsf{x_i}$	$\mathsf{x_j}$	$\mathsf{x_k} = \mathsf{x_i} \wedge \mathsf{x_j}$	CNF clause
0	0	0	1	
0	0	1	1	
0	1	0	1	
0	1	1	0	$\overline{\mathsf{x_k}} \vee \mathsf{x_i} \vee \mathsf{x_j}$
1	0	0	0	$\mathsf{x_k} \vee \overline{\mathsf{x_i}} \vee \overline{\mathsf{x_j}}$
1	0	1	0	$\mathsf{x_k} \vee \overline{\mathsf{x_i}} \vee \mathsf{x_j}$
1	1	0	0	$\mathsf{x_k} \vee \mathsf{x_i} \vee \overline{\mathsf{x_j}}$
1	1	1	1	

The conjunction (i.e., and) of all these clauses is clearly equivalent to the original formula. In this case

$\psi \equiv (\overline{\mathsf{x_k}} \vee \mathsf{x_i} \vee \mathsf{x_j}) \wedge (\mathsf{x_k} \vee \overline{\mathsf{x_i}} \vee \overline{\mathsf{x_j}}) \wedge (\mathsf{x_k} \vee \overline{\mathsf{x_i}} \vee \mathsf{x_j}) \wedge (\mathsf{x_k} \vee \mathsf{x_i} \vee \overline{\mathsf{x_j}})$

Formula conversion into CNF

Step 3 - simplify if you want to

Using that $(x \vee y) \wedge (x \vee \overline{y}) = x$, we have that:

1. $(x_k \vee \overline{x_i} \vee \overline{x_j}) \wedge (x_k \vee \overline{x_i} \vee x_j)$ is equivalent to $(x_k \vee \overline{x_i})$.
2. $(x_k \vee \overline{x_i} \vee \overline{x_j}) \wedge (x_k \vee x_i \vee \overline{x_j})$ is equivalent to $(x_k \vee \overline{x_j})$.

Using the above two observation, we have that our formula
$\psi \equiv (\overline{x_k} \vee x_i \vee x_j) \wedge (x_k \vee \overline{x_i} \vee \overline{x_j}) \wedge (x_k \vee \overline{x_i} \vee x_j) \wedge (x_k \vee x_i \vee \overline{x_j})$
is equivalent to
$\psi \equiv (\overline{x_k} \vee x_i \vee x_j) \wedge (x_k \vee \overline{x_i}) \wedge (x_k \vee \overline{x_j})$.
We conclude:

Lemma

The formula $x_k = x_i \wedge x_j$ *is equivalent to the* CNF *formula*
$\psi \equiv (\overline{x_k} \vee x_i \vee x_j) \wedge (x_k \vee \overline{x_i}) \wedge (x_k \vee \overline{x_j})$.