CS 473: Fundamental Algorithms, Spring 2013

co-NP, Self-Reductions

Lecture 24

April 24, 2013

Part I

Complementation and Self-Reduction

The class P

1. A language $\mathbf{L}$ (equivalently decision problem) is in the class $\mathbf{P}$ if there is a polynomial time algorithm $\mathbf{A}$ for deciding $\mathbf{L}$; that is given a string $\mathbf{x}$, $\mathbf{A}$ correctly decides if $\mathbf{x} \in \mathbf{L}$ and running time of $\mathbf{A}$ on $\mathbf{x}$ is polynomial in $|\mathbf{x}|$, the length of $\mathbf{x}$.

The class NP

Two equivalent definitions:

1. Language $\mathbf{L}$ is in $\mathbf{NP}$ if there is a non-deterministic polynomial time algorithm $\mathbf{A}$ (Turing Machine) that decides $\mathbf{L}$.
    1. For $\mathbf{x} \in \mathbf{L}$, $\mathbf{A}$ has some non-deterministic choice of moves that will make $\mathbf{A}$ accept $\mathbf{x}$
    2. For $\mathbf{x} \notin \mathbf{L}$, no choice of moves will make $\mathbf{A}$ accept $\mathbf{x}$
2. $\mathbf{L}$ has an efficient certifier $\mathbf{C}(\cdot, \cdot)$.
    1. $\mathbf{C}$ is a polynomial time deterministic algorithm
    2. For $\mathbf{x} \in \mathbf{L}$ there is a string $\mathbf{y}$ (proof) of length polynomial in $|\mathbf{x}|$ such that $\mathbf{C}(\mathbf{x}, \mathbf{y})$ accepts
    3. For $\mathbf{x} \notin \mathbf{L}$, no string $\mathbf{y}$ will make $\mathbf{C}(\mathbf{x}, \mathbf{y})$ accept

Complementation

Definition

Given a decision problem $\mathbf{X}$, its **complement** $\overline{\mathbf{X}}$ is the collection of all instances $\mathbf{s}$ such that $\mathbf{s} \notin \mathbf{L(X)}$

Equivalently, in terms of languages:

Definition

Given a language $\mathbf{L}$ over alphabet $\mathbf{\Sigma}$, its **complement** $\overline{\mathbf{L}}$ is the language $\mathbf{\Sigma}^* \setminus \mathbf{L}$.

Examples

1. $\mathbf{PRIME} = \{\mathbf{n} \mid \mathbf{n} \text{ is an integer and } \mathbf{n} \text{ is prime}\}$
   $\overline{\mathbf{PRIME}} = \left\{\mathbf{n} \;\middle|\; \mathbf{n} \text{ is an integer and } \mathbf{n} \text{ is not a prime}\right\}$
   $\overline{\mathbf{PRIME}} = \mathbf{COMPOSITE}$.
2. $\mathbf{SAT} = \left\{\varphi \;\middle|\; \varphi \text{ is a CNF formula and } \varphi \text{ is satisfiable}\right\}$
   $\overline{\mathbf{SAT}} = \left\{\varphi \;\middle|\; \varphi \text{ is a CNF formula and } \varphi \text{ is not satisfiable}\right\}$.
   $\overline{\mathbf{SAT}} = \mathbf{UnSAT}$.

Technicality: $\overline{\mathbf{SAT}}$ also includes strings that do not encode any valid CNF formula. Typically we ignore those strings because they are not interesting. In all problems of interest, we assume that it is "easy" to check whether a given string is a valid instance or not.

P is closed under complementation

Proposition

Decision problem $\mathbf{X}$ *is in* $\mathbf{P}$ *if and only if* $\overline{\mathbf{X}}$ *is in* $\mathbf{P}$.

Proof.

1. If $\mathbf{X}$ is in $\mathbf{P}$ let $\mathbf{A}$ be a polynomial time algorithm for $\mathbf{X}$.
2. Construct polynomial time algorithm $\mathbf{A'}$ for $\overline{\mathbf{X}}$ as follows: given input $\mathbf{x}$, $\mathbf{A'}$ runs $\mathbf{A}$ on $\mathbf{x}$ and if $\mathbf{A}$ accepts $\mathbf{x}$, $\mathbf{A'}$ rejects $\mathbf{x}$ and if $\mathbf{A}$ rejects $\mathbf{x}$ then $\mathbf{A'}$ accepts $\mathbf{x}$.
3. Only if direction is essentially the same argument.

$\square$

Asymmetry of NP

Definition

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

Observation

To show that a problem is in **NP** we only need short, efficiently checkable certificates for "yes"-instances. What about "no"-instances?

Given a CNF formula φ, is φ unsatisfiable?

Easy to give a proof that φ is satisfiable (an assignment) but no easy (known) proof to show that φ is unsatisfiable!

Examples of complement problems

Some languages

1. **UnSAT**: CNF formulas φ that are not satisfiable
2. **No-Hamilton-Cycle**: graphs $\mathbf{G}$ that do not have a Hamilton cycle
3. **No-3-Color**: graphs $\mathbf{G}$ that are not 3-colorable

Above problems are complements of known **NP** problems (viewed as languages).

NP and co-NP

NP

Decision problems with a polynomial certifier.
Examples: **SAT**, **Hamiltonian Cycle**, **3-Colorability**.

Definition

co-NP is the class of all decision problems $\mathbf{X}$ such that $\overline{\mathbf{X}} \in \mathbf{NP}$.
Examples: **UnSAT**, **No-Hamiltonian-Cycle**, **No-3-Colorable**.

co-NP

If $\mathbf{L}$ is a language in **co-NP** then that there is a polynomial time certifier/verifier $\mathbf{C}(\cdot, \cdot)$, such that:

1. for $\mathbf{s} \not\in \mathbf{L}$ there is a proof $\mathbf{t}$ of size polynomial in $|\mathbf{s}|$ such that $\mathbf{C}(\mathbf{s}, \mathbf{t})$ correctly says NO.
2. for $\mathbf{s} \in \mathbf{L}$ there is no proof $\mathbf{t}$ for which $\mathbf{C}(\mathbf{s}, \mathbf{t})$ will say NO

co-NP has checkable proofs for strings NOT in the language.

Natural Problems in co-NP

1. **Tautology**: given a Boolean formula (not necessarily in CNF form), is it true for *all* possible assignments to the variables?
2. **Graph expansion**: given a graph $\mathbf{G}$, is it an *expander*? A graph $\mathbf{G} = (\mathbf{V}, \mathbf{E})$ is an **expander** if and only if for each $\mathbf{S} \subset \mathbf{V}$ with $|\mathbf{S}| \leq |\mathbf{V}|/2$, $|\mathbf{N}(\mathbf{S})| \geq |\mathbf{S}|$. Expanders are very important graphs in theoretical computer science and mathematics.

Factorization, Primality

Problem: **Primality**

Instance: An integer $\mathbf{n}$.
Question: Is the number $\mathbf{n}$ prime?

Problem: **Factoring**

Instance: Integers $\mathbf{n}, \mathbf{k}$.
Question: Does the number $\mathbf{n}$ has a factor $\leq \mathbf{k}$? Formally, is there ℓ, such that $\mathbf{2} \leq \ell \leq \mathbf{k}$, such that ℓ divides $\mathbf{n}$?

1. **Primality** is in **P**.
2. **Factoring** is in $\mathbf{NP} \cap \mathbf{co\text{-}NP}$.

Factoring is a very naughty problem

Problem: **Factoring**

Instance: Integers $\mathbf{n}, \mathbf{k}$.
Question: Does the number $\mathbf{n}$ has a factor $\leq \mathbf{k}$? Formally, is there ℓ, such that $\mathbf{2} \leq \ell \leq \mathbf{k}$, such that ℓ divides $\mathbf{n}$?

If answer is:

1. NO: certificate is all prime factors of $\mathbf{n}$. Certification: multiply the given numbers.
2. YES: Certificate is the factor ℓ. Verify it divides $\mathbf{n}$.

Belief: Unlikely **Factoring** is **NP-Complete**. Can be solved in polynomial time on a quantum computer.

P, NP, co-NP

co-P: complement of P. Language $\mathbf{X}$ is in **co-P** iff $\overline{\mathbf{X}} \in \mathbf{P}$

Proposition

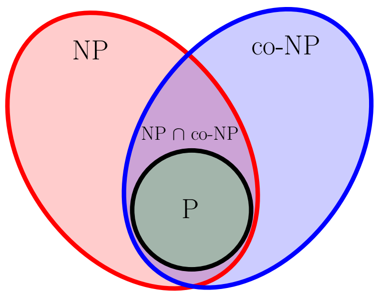
$\mathbf{P} = \mathbf{co\text{-}P}$.

Proposition

$\mathbf{P} \subseteq \mathbf{NP} \cap \mathbf{co\text{-}NP}$.

Saw that $\mathbf{P} \subseteq \mathbf{NP}$. Same proof shows $\mathbf{P} \subseteq \mathbf{co\text{-}NP}$.

P, NP, and co-NP



Open Problems:

1. Does $\mathbf{NP} = \mathbf{co\text{-}NP}$?
   Consensus opinion: No.
2. Is $\mathbf{P} = \mathbf{NP} \cap \mathbf{co\text{-}NP}$?
   No real consensus.

P, NP, and co-NP

Proposition

If $\mathbf{P} = \mathbf{NP}$ *then* $\mathbf{NP} = \mathbf{co\text{-}NP}$.

Proof.

$\mathbf{P} = \mathbf{co\text{-}P}$

If $\mathbf{P} = \mathbf{NP}$ then $\mathbf{co\text{-}NP} = \mathbf{co\text{-}P} = \mathbf{P}$. □

P, NP, and co-NP

Which means that...

Corollary

If $\mathbf{NP} \neq \mathbf{co\text{-}NP}$ *then* $\mathbf{P} \neq \mathbf{NP}$.

Importance of corollary: try to prove $\mathbf{P} \neq \mathbf{NP}$ by proving that $\mathbf{NP} \neq \mathbf{co\text{-}NP}$.

NP ∩ co-NP

Complexity Class NP ∩ co-NP

Problems in this class have

1. Efficient certifiers for yes-instances
2. Efficient disqualifiers for no-instances

Problems have a good characterization property, since for both yes and no instances we have short efficiently checkable proofs.

NP ∩ co-NP: Example

Example

Bipartite Matching: Given bipartite graph $\mathbf{G} = (\mathbf{U} \cup \mathbf{V}, \mathbf{E})$, does $\mathbf{G}$ have a perfect matching?

Bipartite Matching $\in \mathbf{NP} \cap \mathbf{co\text{-}NP}$

1. If $\mathbf{G}$ is a yes-instance, then proof is just the perfect matching.
2. If $\mathbf{G}$ is a no-instance, then by Hall's Theorem, there is a subset of vertices $\mathbf{A} \subseteq \mathbf{U}$ such that $|\mathbf{N}(\mathbf{A})| < |\mathbf{A}|$.

Example (More interesting...)

Factoring $\in \mathbf{NP} \cap \mathbf{co\text{-}NP}$, and we do not know if it is in $\mathbf{P}$!

Good Characterization $\stackrel{?}{=}$ Efficient Solution

1. Bipartite Matching has a polynomial time algorithm
2. Do all problems in **NP** $\cap$ **co-NP** have polynomial time algorithms? That is, is **P** = **NP** $\cap$ **co-NP**?
   Problems in **NP** $\cap$ **co-NP** have been proved to be in **P** many years later
   1. Linear programming (Khachiyan 1979)
      1. Duality easily shows that it is in **NP** $\cap$ **co-NP**
   2. Primality Testing (Agarwal-Kayal-Saxena 2002)
      1. Easy to see that **PRIME** is in **co-NP** (why?)
      2. **PRIME** is in **NP** - not easy to show! (Vaughan Pratt 1975)

P $\stackrel{?}{=}$ NP $\cap$ co-NP (contd)

1. Some problems in **NP** $\cap$ **co-NP** still cannot be proved to have polynomial time algorithms
   1. Parity Games.
   2. Other more specialized problems.

co-NP Completeness

Definition

A problem **X** is said to be co-NP-Complete (**co-NPC**) if

1. **X** $\in$ **co-NP**
2. (Hardness) For any **Y** $\in$ **co-NP**, **Y** $\leq_P$ **X**

co-NP-Complete problems are the hardest problems in **co-NP**.

Lemma

X is co-NPC if and only if $\overline{\mathbf{X}}$ *is NP-Complete.*

Proof left as an exercise.

P, NP and co-NP

Possible scenarios:

1. **P** = **NP**. Then **P** = **NP** = **co-NP**.
2. **NP** = **co-NP** and **P** $\neq$ **NP** (and hence also **P** $\neq$ **co-NP**).
3. **NP** $\neq$ **co-NP**. Then **P** $\neq$ **NP** and also **P** $\neq$ **co-NP**.

Most people believe that the last scenario is the likely one.

Question: Suppose **P** $\neq$ **NP**. Is every problem that is in **NP** $\setminus$ **P** is also **NP-Complete**?

Theorem (Ladner)

If **P** $\neq$ **NP** *then there is a problem/language* **X** $\in$ **NP** $\setminus$ **P** *such that* **X** *is not* **NP-Complete**.

Karp vs Turing Reduction and NP vs co-NP

Question: Why restrict to Karp reductions for NP-Completeness?

Lemma

*If $\mathbf{X} \in$ **co-NP** and $\mathbf{Y}$ is **NP-Complete** then $\mathbf{X} \leq_{\mathbf{P}} \mathbf{Y}$ under Turing reduction.*

Thus, Turing reductions cannot distinguish **NP** and **co-NP**.

Back to Decision versus Search

1. Recall, decision problems are those with yes/no answers, while search problems require an explicit solution for a yes instance

Example

1. Satisfiability
   1. Decision: Is the formula φ satisfiable?
   2. Search: Find assignment that satisfies φ
2. Graph coloring
   1. Decision: Is graph $\mathbf{G}$ 3-colorable?
   2. Search: Find a 3-coloring of the vertices of $\mathbf{G}$

Decision "reduces to" Search

1. Efficient algorithm for search implies efficient algorithm for decision.
2. If decision problem is difficult then search problem is also difficult.
3. Can an efficient algorithm for decision imply an efficient algorithm for search?
   Yes, for all the problems we have seen. In fact for all **NP-Complete** Problems.

Self Reduction

Definition

A problem is said to be **self reducible** if the search problem reduces (by Turing reduction) in polynomial time to decision problem. In other words, there is an algorithm to solve the search problem that has polynomially many steps, where each step is either

1. A conventional computational step, or
2. a call to subroutine solving the decision problem.

Back to SAT

Proposition

SAT *is self reducible.*

In other words, there is a polynomial time algorithm to find the satisfying assignment if one can periodically check if some formula is satisfiable.

Search Algorithm for SAT

given a Decision Algorithm for **SAT**

Input: **SAT** formula φ with $\mathbf{n}$ variables $\mathbf{x_1, x_2, \ldots, x_n}$.

1. set $\mathbf{x_1 = 0}$ in φ and get new formula φ_1. check if φ_1 is satisfiable using decision algorithm. if φ_1 is satisfiable, recursively find assignment to $\mathbf{x_2, x_3, \ldots, x_n}$ that satisfy φ_1 and output $\mathbf{x_1 = 0}$ along with the assignment to $\mathbf{x_2, \ldots, x_n}$.
2. if φ_1 is not satisfiable then set $\mathbf{x_1 = 1}$ in φ to get formula φ_2. if φ_2 is satisfiable , recursively find assignment to $\mathbf{x_2, x_3, \ldots, x_n}$ that satisfy φ_2 and output $\mathbf{x_1 = 1}$ along with the assignment to $\mathbf{x_2, \ldots, x_n}$.
3. if φ_1 and φ_2 are both not satisfiable then φ is not satisfiable.

Algorithm runs in polynomial time if the decision algorithm for **SAT** runs in polynomial time. At most $\mathbf{2n}$ calls to decision algorithm.

Self-Reduction for NP-Complete Problems

Theorem

Every **NP-Complete** *problem/language* $\mathbf{L}$ *is self-reducible.*

Proof is not hard but requires understanding of proof of Cook-Levin theorem.

Note that proof is only for complete languages, not for all languages in **NP**. Otherwise **Factoring** would be in polynomial time and we would not rely on it for our current security protocols.

Easy and instructive to prove self-reducibility for specific **NP-Complete** problems such as **Independent Set**, **Vertex Cover**, **Hamiltonian Cycle**, etc.
See discussion section problems.