CS 573: Algorithms, Fall 2013

NP Completeness

Lecture 3

September 3, 2013

Part I

NP Completeness

Certifiers

Definition

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

Definition (Efficient Certifier.)

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

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

NP-Complete Problems

Definition

A problem X is said to be **NP-Complete** if

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

Solving NP-Complete Problems

Proposition

Suppose X is **NP-Complete**. *Then X can be solved in polynomial time if and only if* $\mathbf{P} = \mathbf{NP}$.

Proof.

$\Rightarrow$ Suppose X can be solved in polynomial time

1. Let $Y \in \mathbf{NP}$. We know $Y \leq_P X$.
2. We showed that if $Y \leq_P X$ and X can be solved in polynomial time, then Y can be solved in polynomial time.
3. Thus, every problem $Y \in \mathbf{NP}$ is such that $Y \in P$; $NP \subseteq P$.
4. Since $\mathbf{P} \subseteq \mathbf{NP}$, we have $\mathbf{P} = \mathbf{NP}$.

$\Leftarrow$ Since $\mathbf{P} = \mathbf{NP}$, and $X \in \mathbf{NP}$, we have a polynomial time algorithm for X. □

NP-Hard Problems

Definition

A problem X is said to be **NP-Hard** if

1. (Hardness) For any $Y \in \mathbf{NP}$, we have that $Y \leq_P X$.

An **NP-Hard** problem need not be in **NP**!

Example: Halting problem is **NP-Hard** (why?) but not **NP-Complete**.

Consequences of proving NP-Completeness

If X is **NP-Complete**

1. Since we believe $\mathbf{P} \neq \mathbf{NP}$,
2. and solving X implies $\mathbf{P} = \mathbf{NP}$.

X is unlikely to be efficiently solvable.

At the very least, many smart people before you have failed to find an efficient algorithm for X.
(This is proof by mob opinion — take with a grain of salt.)

NP-Complete Problems

Question

Are there any problems that are **NP-Complete**?

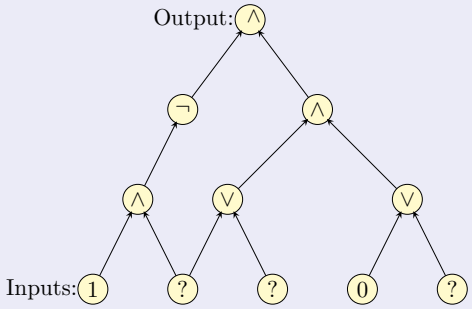
Answer

Yes! Many, many problems are **NP-Complete**.

Circuits

Definition

A circuit is a directed *acyclic* graph with



1. Input vertices (without incoming edges) labelled with $\mathbf{0}$, $\mathbf{1}$ or a distinct variable.
2. Every other vertex is labelled $\vee$, $\wedge$ or $\neg$.
3. Single node output vertex with no outgoing edges.

Cook-Levin Theorem

Definition (Circuit Satisfaction (CSAT).)

Given a circuit as input, is there an assignment to the input variables that causes the output to get value $\mathbf{1}$?

Theorem (Cook-Levin)

CSAT is **NP-Complete**.

Need to show

1. **CSAT** is in **NP**.
2. *every* **NP** problem X reduces to **CSAT**.

CSAT: Circuit Satisfaction

Claim

CSAT is in **NP**.

1. Certificate: Assignment to input variables.
2. Certifier: Evaluate the value of each gate in a topological sort of DAG and check the output gate value.

CSAT is NP-hard: Idea

Need to show that *every* **NP** problem X reduces to **CSAT**.

What does it mean that $X \in$ **NP**?

$X \in$ **NP** implies that there are polynomials $p()$ and $q()$ and certifier/verifier program C such that for every string s the following is true:

1. If s is a YES instance ($s \in X$) then there is a *proof* t of length $p(|s|)$ such that $C(s, t)$ says YES.
2. If s is a NO instance ($s \notin X$) then for every string t of length at $p(|s|)$, $C(s, t)$ says NO.
3. $C(s, t)$ runs in time $q(|s| + |t|)$ time (hence polynomial time).

Reducing X to CSAT

X is in **NP** means we have access to $p(), q(), C(\cdot,\cdot)$.
What is $C(\cdot,\cdot)$? It is a program or equivalently a Turing Machine!
How are $p()$ and $q()$ given? As numbers.
Example: if 3 is given then $p(n) = n^3$.

Thus an **NP** problem is essentially a three tuple $\langle p, q, C\rangle$ where C is either a program or a TM.

Reducing X to CSAT

Thus an **NP** problem is essentially a three tuple $\langle p, q, C\rangle$ where C is either a program or TM.

Problem X: Given string s, is $s \in X$?

Same as the following: is there a proof t of length $p(|s|)$ such that $C(s,t)$ says YES.

How do we reduce X to **CSAT**? Need an algorithm $\mathcal{A}$ that

1. takes s (and $\langle p, q, C\rangle$) and creates a circuit G in polynomial time in $|s|$ (note that $\langle p, q, C\rangle$ are fixed).
2. G is satisfiable if and only if there is a proof t such that $C(s,t)$ says YES.

Reducing X to CSAT

How do we reduce X to **CSAT**? Need an algorithm $\mathcal{A}$ that

1. takes s (and $\langle p, q, C\rangle$) and creates a circuit G in polynomial time in $|s|$ (note that $\langle p, q, C\rangle$ are fixed).
2. G is satisfiable if and only if there is a proof t such that $C(s,t)$ says YES

Simple but Big Idea: Programs are essentially the same as Circuits!

1. Convert $C(s,t)$ into a circuit G with t as unknown inputs (rest is known including s)
2. We know that $|t| = p(|s|)$ so express boolean string t as $p(|s|)$ variables $t_1, t_2, \ldots, t_k$ where $k = p(|s|)$.
3. Asking if there is a proof t that makes $C(s,t)$ say YES is same as whether there is an assignment of values to "unknown" variables $t_1, t_2, \ldots, t_k$ that will make G evaluate to true/YES.

Example: Independent Set

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

Formally, why is **Independent Set** in **NP**?

Example: Independent Set

Formally why is **Independent Set** in **NP**?

1. Input: $< n, y_{1,1}, y_{1,2}, \ldots, y_{1,n}, y_{2,1}, \ldots, y_{2,n}, \ldots, y_{n,1}, \ldots, y_{n,n}, k >$ encodes $< G, k >$.
   1. n is number of vertices in G
   2. $y_{i,j}$ is a bit which is 1 if edge (i, j) is in G and 0 otherwise (adjacency matrix representation)
   3. k is size of independent set.
2. Certificate: $t = t_1 t_2 \ldots t_n$. Interpretation is that t_i is 1 if vertex i is in the independent set, 0 otherwise.

Certifier for Independent Set

Certifier $C(s, t)$ for **Independent Set**:

```
if (t_1 + t_2 + ... + t_n < k) then
    return NO
else
    for each (i, j) do
        if (t_i ∧ t_j ∧ y_{i,j}) then
            return NO

return YES
```


Example: Independent Set

A certifier circuit for Independent Set

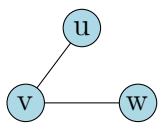
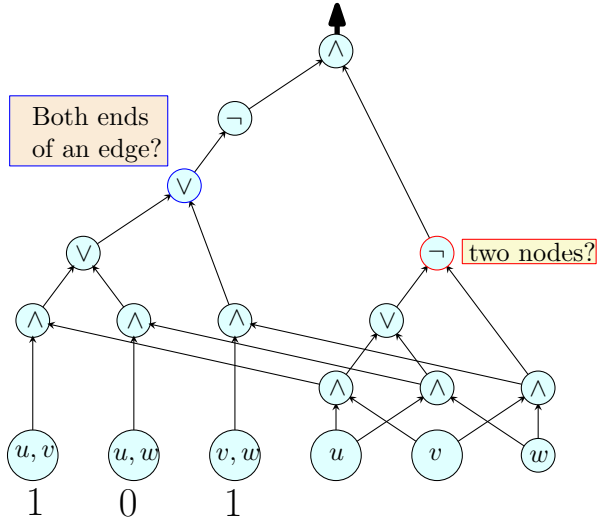


Figure : Graph G with $k = 2$



Programs, Turing Machines and Circuits

Consider "program" A that takes $f(|s|)$ steps on input string s.

Question: What computer is the program running on and what does *step* mean?

Real computers difficult to reason with mathematically because

1. instruction set is too rich
2. pointers and control flow jumps in one step
3. assumption that pointer to code fits in one word

Turing Machines

1. simpler model of computation to reason with
2. can simulate real computers with *polynomial* slow down
3. all moves are *local* (head moves only one cell)

Certifiers that at TMs

Assume $C(\cdot,\cdot)$ is a (deterministic) Turing Machine M

Problem: Given M, input s, p, q decide if there is a proof t of length $p(|s|)$ such that M on s, t will halt in $q(|s|)$ time and say YES.

There is an algorithm $\mathcal{A}$ that can reduce above problem to **CSAT** mechanically as follows.

1. $\mathcal{A}$ first computes $p(|s|)$ and $q(|s|)$.
2. Knows that M can use at most $q(|s|)$ memory/tape cells
3. Knows that M can run for at most $q(|s|)$ time
4. Simulates the evolution of the state of M and memory over time using a big circuit.

Simulation of Computation via Circuit

1. Think of M's state at time ℓ as a string $x^\ell = x_1 x_2 \ldots x_k$ where each $x_i \in \{0, 1, B\} \times Q \cup \{q_{-1}\}$.
2. At time 0 the state of M consists of input string s a guess t (unknown variables) of length $p(|s|)$ and rest $q(|s|)$ blank symbols.
3. At time $q(|s|)$ we wish to know if M stops in q_{accept} with say all blanks on the tape.
4. We write a circuit C_ℓ which captures the transition of M from time ℓ to time $\ell + 1$.
5. Composition of the circuits for all times 0 to $q(|s|)$ gives a big (still poly) sized circuit $\mathcal{C}$
6. The final output of $\mathcal{C}$ should be true if and only if the entire state of M at the end leads to an accept state.

NP-Hardness of Circuit Satisfaction

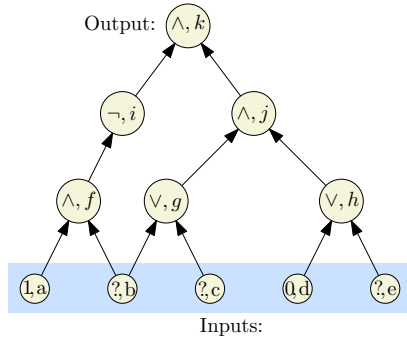
Key Ideas in reduction:

1. Use TMs as the code for certifier for simplicity
2. Since $p()$ and $q()$ are known to $\mathcal{A}$, it can set up all required memory and time steps in advance
3. Simulate computation of the TM from one time to the next as a circuit that only looks at three adjacent cells at a time

Note: Above reduction can be done to **SAT** as well. Reduction to **SAT** was the original proof of Steve Cook.

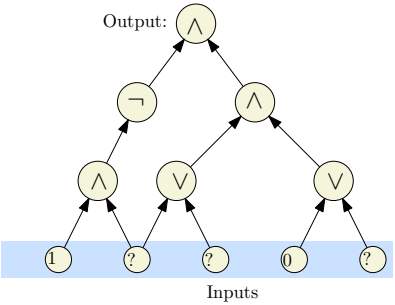
SAT is NP-Complete

1. We have seen that **SAT** $\in$ **NP**
2. To show **NP-Hardness**, we will reduce Circuit Satisfiability (**CSAT**) to **SAT**
   Instance of **CSAT** (we label each node):

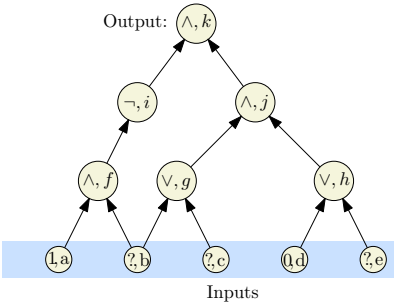


Converting a circuit into a CNF formula

Label the nodes



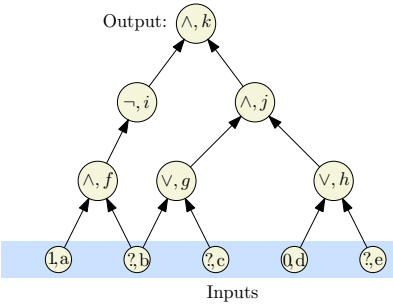
(A) Input circuit



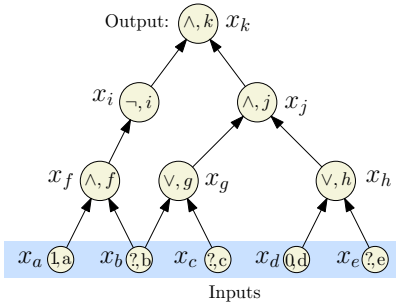
(B) Label the nodes.

Converting a circuit into a CNF formula

Introduce a variable for each node



(B) Label the nodes.

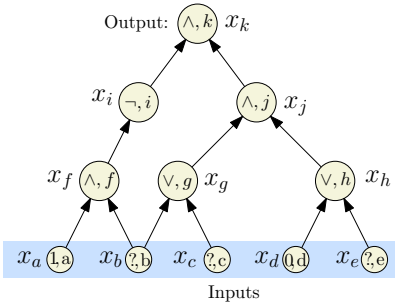


(C) Introduce var for each node.

Converting a circuit into a CNF formula

Write a sub-formula for each variable that is true if the var is computed correctly.

XXX



(C) Introduce var for each node.

x_k (Demand a sat' assignment!)

$x_k = x_i \wedge x_k$

$x_j = x_g \wedge x_h$

$x_i = \neg x_f$

$x_h = x_d \vee x_e$

$x_g = x_b \vee x_c$

$x_f = x_a \wedge x_b$

$x_d = 0$

$x_a = 1$

(D) Write a sub-formula for each variable that is true if the var is computed correctly.

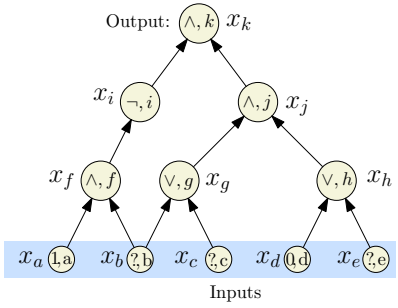
Converting a circuit into a CNF formula

Convert each sub-formula to an equivalent CNF formula

x_k	x_k
$x_k = x_i \wedge x_j$	$(\neg x_k \vee x_i) \wedge (\neg x_k \vee x_j) \wedge (x_k \vee \neg x_i \vee \neg x_j)$
$x_j = x_g \wedge x_h$	$(\neg x_j \vee x_g) \wedge (\neg x_j \vee x_h) \wedge (x_j \vee \neg x_g \vee \neg x_h)$
$x_i = \neg x_f$	$(x_i \vee x_f) \wedge (\neg x_i \vee \neg x_f)$
$x_h = x_d \vee x_e$	$(x_h \vee \neg x_d) \wedge (x_h \vee \neg x_e) \wedge (\neg x_h \vee x_d \vee x_e)$
$x_g = x_b \vee x_c$	$(x_g \vee \neg x_b) \wedge (x_g \vee \neg x_c) \wedge (\neg x_g \vee x_b \vee x_c)$
$x_f = x_a \wedge x_b$	$(\neg x_f \vee x_a) \wedge (\neg x_f \vee x_b) \wedge (x_f \vee \neg x_a \vee \neg x_b)$
$x_d = 0$	$\neg x_d$
$x_a = 1$	x_a

Converting a circuit into a CNF formula

Take the conjunction of all the CNF sub-formulas



$$
\begin{aligned}
& x_k \wedge (\neg x_k \vee x_i) \wedge (\neg x_k \vee x_j) \\
& \wedge (x_k \vee \neg x_i \vee \neg x_j) \wedge (\neg x_j \vee x_g) \\
& \wedge (\neg x_j \vee x_h) \wedge (x_j \vee \neg x_g \vee \neg x_h) \\
& \wedge (x_i \vee x_f) \wedge (\neg x_i \vee \neg x_f) \\
& \wedge (x_h \vee \neg x_d) \wedge (x_h \vee \neg x_e) \\
& \wedge (\neg x_h \vee x_d \vee x_e) \wedge (x_g \vee \neg x_b) \\
& \wedge (x_g \vee \neg x_c) \wedge (\neg x_g \vee x_b \vee x_c) \\
& \wedge (\neg x_f \vee x_a) \wedge (\neg x_f \vee x_b) \\
& \wedge (x_f \vee \neg x_a \vee \neg x_b) \wedge (\neg x_d) \wedge x_a
\end{aligned}
$$

We got a CNF formula that is satisfiable if and only if the original circuit is satisfiable.

Reduction: CSAT $\leq_P$ SAT

1. For each gate (vertex) v in the circuit, create a variable x_v
2. Case $\neg$: v is labeled $\neg$ and has one incoming edge from u (so $x_v = \neg x_u$). In **SAT** formula generate, add clauses $(x_u \vee x_v)$, $(\neg x_u \vee \neg x_v)$. Observe that

$$x_v = \neg x_u \text{ is true} \iff \begin{matrix} (x_u \vee x_v) \\ (\neg x_u \vee \neg x_v) \end{matrix} \text{ both true.}$$

Reduction: CSAT $\leq_P$ SAT

Continued...

1. Case $\vee$: So $x_v = x_u \vee x_w$. In **SAT** formula generated, add clauses $(x_v \vee \neg x_u)$, $(x_v \vee \neg x_w)$, and $(\neg x_v \vee x_u \vee x_w)$. Again, observe that

$$\left(x_v = x_u \vee x_w\right) \text{ is true} \iff \begin{matrix} (x_v \vee \neg x_u), \\ (x_v \vee \neg x_w), \\ (\neg x_v \vee x_u \vee x_w) \end{matrix} \text{ all true.}$$

Reduction: CSAT $\leq_P$ SAT

Continued...

1. Case $\wedge$: So $x_v = x_u \wedge x_w$. In **SAT** formula generated, add clauses $(\neg x_v \vee x_u)$, $(\neg x_v \vee x_w)$, and $(x_v \vee \neg x_u \vee \neg x_w)$. Again observe that

$$x_v = x_u \wedge x_w \text{ is true} \iff \begin{matrix} (\neg x_v \vee x_u), \\ (\neg x_v \vee x_w), \\ (x_v \vee \neg x_u \vee \neg x_w) \end{matrix} \text{ all true.}$$

Reduction: CSAT $\leq_P$ SAT

Continued...

1. If v is an input gate with a fixed value then we do the following. If $x_v = 1$ add clause x_v. If $x_v = 0$ add clause $\neg x_v$
2. Add the clause x_v where v is the variable for the output gate

Correctness of Reduction

Need to show circuit C is satisfiable iff φ_C is satisfiable

$\Rightarrow$ Consider a satisfying assignment a for C

1. Find values of all gates in C under a
2. Give value of gate v to variable x_v; call this assignment a'
3. a' satisfies φ_C (exercise)

$\Leftarrow$ Consider a satisfying assignment a for φ_C

1. Let a' be the restriction of a to only the input variables
2. Value of gate v under a' is the same as value of x_v in a
3. Thus, a' satisfies C

Theorem

SAT is **NP-Complete**.

Proving that a problem X is NP-Complete

To prove X is **NP-Complete**, show

1. Show X is in **NP**.
   1. certificate/proof of polynomial size in input
   2. polynomial time certifier $C(s, t)$
2. Reduction from a known **NP-Complete** problem such as **CSAT** or **SAT** to X

SAT $\leq_P$ X implies that every **NP** problem $Y \leq_P X$. Why?
Transitivity of reductions:

$Y \leq_P SAT$ and $SAT \leq_P X$ and hence $Y \leq_P X$.

NP-Completeness via Reductions

1. **CSAT** is **NP-Complete**.
2. **CSAT** $\leq_P$ **SAT** and **SAT** is in **NP** and hence **SAT** is **NP-Complete**.
3. **SAT** $\leq_P$ **3-SAT** and hence 3-SAT is **NP-Complete**.
4. **3-SAT** $\leq_P$ **Independent Set** (which is in **NP**) and hence **Independent Set** is **NP-Complete**.
5. **Vertex Cover** is **NP-Complete**.
6. **Clique** is **NP-Complete**.

Hundreds and thousands of different problems from many areas of science and engineering have been shown to be **NP-Complete**.

A surprisingly frequent phenomenon!