NP Completeness and Cook-Levin Theorem

Lecture 22

November 18, 2014

P and **NP** and Turing Machines

1. **P**: set of decision problems that have polynomial time algorithms.
2. **NP**: set of decision problems that have polynomial time non-deterministic algorithms.

Question: What is an algorithm? Depends on the model of computation!

What is our model of computation?

Formally speaking our model of computation is Turing Machines.

P and **NP** and Turing Machines

1. **P**: set of decision problems that have polynomial time algorithms.
2. **NP**: set of decision problems that have polynomial time non-deterministic algorithms.

Question: What is an algorithm? Depends on the model of computation!

What is our model of computation?

Formally speaking our model of computation is Turing Machines.

P and **NP** and Turing Machines

1. **P**: set of decision problems that have polynomial time algorithms.
2. **NP**: set of decision problems that have polynomial time non-deterministic algorithms.

Question: What is an algorithm? Depends on the model of computation!

What is our model of computation?

Formally speaking our model of computation is Turing Machines.

P and **NP** and Turing Machines

1. **P**: set of decision problems that have polynomial time algorithms.
2. **NP**: set of decision problems that have polynomial time non-deterministic algorithms.

Question: What is an algorithm? Depends on the model of computation!

What is our model of computation?

Formally speaking our model of computation is Turing Machines.

P and **NP** and Turing Machines

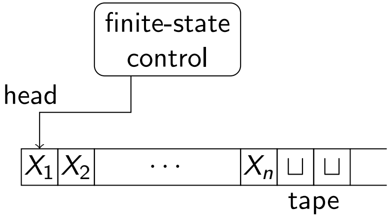
1. **P**: set of decision problems that have polynomial time algorithms.
2. **NP**: set of decision problems that have polynomial time non-deterministic algorithms.

Question: What is an algorithm? Depends on the model of computation!

What is our model of computation?

Formally speaking our model of computation is Turing Machines.

Turing Machines: Recap



1. Infinite tape.
2. Finite state control.
3. Input at beginning of tape.
4. Special tape letter "blank" $\sqcup$.
5. Head can move only one cell to left or right.

Turing Machines: Formally

A TM $\mathbf{M} = (\mathbf{Q}, \mathbf{\Sigma}, \mathbf{\Gamma}, \delta, \mathbf{q_0}, \mathbf{q_{accept}}, \mathbf{q_{reject}})$:

1. $\mathbf{Q}$ is set of states in finite control
2. $\mathbf{q_0}$ start state, $\mathbf{q_{accept}}$ is accept state, $\mathbf{q_{reject}}$ is reject state
3. $\mathbf{\Sigma}$ is input alphabet, $\mathbf{\Gamma}$ is tape alphabet (includes $\sqcup$)
4. $\delta : \mathbf{Q} \times \mathbf{\Gamma} \rightarrow \{\mathbf{L}, \mathbf{R}\} \times \mathbf{\Gamma} \times \mathbf{Q}$ is transition function
    1. $\delta(\mathbf{q}, \mathbf{a}) = (\mathbf{q'}, \mathbf{b}, \mathbf{L})$ means that $\mathbf{M}$ in state $\mathbf{q}$ and head seeing $\mathbf{a}$ on tape will move to state $\mathbf{q'}$ while replacing $\mathbf{a}$ on tape with $\mathbf{b}$ and head moves left.

$\mathbf{L(M)}$: language accepted by $\mathbf{M}$ is set of all input strings $\mathbf{s}$ on which $\mathbf{M}$ accepts; that is:

1. TM is started in state $\mathbf{q_0}$.
2. Initially, the tape head is located at the first cell.
3. The tape contain $\mathbf{s}$ on the tape followed by blanks.
4. The TM halts in the state $\mathbf{q_{accept}}$.

$\mathbf{P}$ via TMs

Definition

$\mathbf{M}$ is a polynomial time TM if there is some polynomial $\mathbf{p}(\cdot)$ such that on all inputs $\mathbf{w}$, $\mathbf{M}$ halts in $\mathbf{p}(|\mathbf{w}|)$ steps.

Definition

$\mathbf{L}$ is a language in $\mathbf{P}$ iff there is a polynomial time TM $\mathbf{M}$ such that $\mathbf{L} = \mathbf{L}(\mathbf{M})$.

NP via TMs

Definition

$\mathbf{L}$ is an **NP** language iff there is a *non-deterministic* polynomial time TM $\mathbf{M}$ such that $\mathbf{L} = \mathbf{L(M)}$.

Non-deterministic TM: each step has a choice of moves

1. $\delta : Q \times \Gamma \rightarrow \mathcal{P}(Q \times \Gamma \times \{L, R\})$.
    1. Example: $\delta(q, a) = \{(q_1, b, L), (q_2, c, R), (q_3, a, R)\}$ means that M can non-deterministically choose one of the three possible moves from (q, a).
2. $L(M)$: set of all strings s on which there *exists* some sequence of valid choices at each step that lead from q_0 to q_{accept}

NP via TMs

Definition

$\mathbf{L}$ is an **NP** language iff there is a *non-deterministic* polynomial time TM $\mathbf{M}$ such that $\mathbf{L = L(M)}$.

Non-deterministic TM: each step has a choice of moves

1. $\delta : Q \times \Gamma \rightarrow \mathcal{P}(Q \times \Gamma \times \{L, R\})$.
   1. Example: $\delta(q, a) = \{(q_1, b, L), (q_2, c, R), (q_3, a, R)\}$ means that $\mathbf{M}$ can non-deterministically choose one of the three possible moves from (q, a).
2. $\mathbf{L(M)}$: set of all strings $\mathbf{s}$ on which there *exists* some sequence of valid choices at each step that lead from q_0 to q_{accept}

Non-deterministic TMs vs certifiers

Two definition of **NP**:

1. **L** is in **NP** iff **L** has a polynomial time certifier $\mathbf{C}(\cdot, \cdot)$.
2. **L** is in **NP** iff **L** is decided by a non-deterministic polynomial time TM **M**.

Claim

Two definitions are equivalent.

Why?

Informal proof idea: the certificate **t** for **C** corresponds to non-deterministic choices of **M** and vice-versa.

In other words **L** is in **NP** iff **L** is accepted by a NTM which first guesses a proof **t** of length poly in input $|\mathbf{s}|$ and then acts as a *deterministic* TM.

Non-determinism, guessing and verification

1. A non-deterministic machine has choices at each step and accepts a string if there *exists* a set of choices which lead to a final state.
2. Equivalently the choices can be thought of as *guessing* a solution and then *verifying* that solution. In this view all the choices are made a priori and hence the verification can be deterministic. The "guess" is the "proof" and the "verifier" is the "certifier".
3. We reemphasize the asymmetry inherent in the definition of non-determinism. Strings in the language can be easily verified. No easy way to verify that a string is not in the language.

Algorithms: TMs vs RAM Model

Why do we use TMs some times and RAM Model other times?

1. TMs are very simple: no complicated instruction set, no jumps/pointers, no explicit loops etc.
    1. Simplicity is useful in proofs.
    2. The "right" formal bare-bones model when dealing with subtleties.
2. RAM model is a closer approximation to the running time/space usage of realistic computers for reasonable problem sizes
    1. Not appropriate for certain kinds of formal proofs when algorithms can take super-polynomial time and space

"Hardest" Problems

Question

What is the hardest problem in **NP**? How do we define it?

Towards a definition

1. Hardest problem must be in **NP**.
2. Hardest problem must be at least as "difficult" as every other problem in **NP**.

What is the hardest question in **P**?

Consider the class **P**. The hardest problem in **P** is:

(A) **Max-Flow**.

(B) **Linear programming**.

(C) **SAT**.

(D) All problems in **P** are easy.

(E) All problems in **P** are hard.

NP-Complete Problems

Definition

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

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

Solving **NP-Complete** Problems

Proposition

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

Proof.

$\Rightarrow$ Suppose $\mathbf{X}$ can be solved in polynomial time

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

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

NP-Hard Problems

Definition

A problem $\mathbf{X}$ is said to be **NP-Hard** if

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

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.)

Consequences of proving **NP-Complete**ness

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.)

Consequences of proving **NP-Complete**ness

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.)

Consequences of proving **NP-Complete**ness

If **X** is **NP-Complete**

1. Since we believe **P** $\neq$ **NP**,
2. and solving **X** implies **P** $=$ **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**?

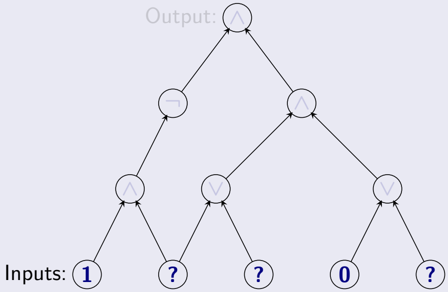
Answer

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

Circuits

Definition

A circuit is a directed *acyclic* graph with

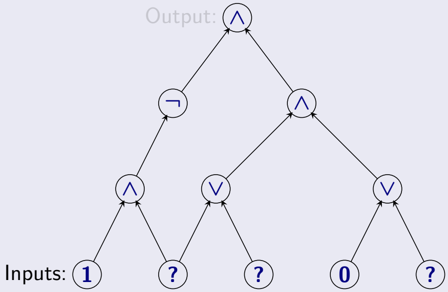


1. Input vertices (without incoming edges) labelled with **0**, **1** or a distinct variable.
2. Every other vertex is labelled $\vee$, $\wedge$ or $\neg$.
3. Single node output vertex with no outgoing edges.

Circuits

Definition

A circuit is a directed *acyclic* graph with

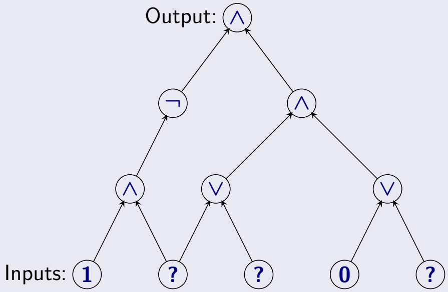


1. Input vertices (without incoming edges) labelled with **0**, **1** or a distinct variable.
2. Every other vertex is labelled $\vee$, $\wedge$ or $\neg$.
3. Single node output vertex with no outgoing edges.

Circuits

Definition

A circuit is a directed *acyclic* graph with



1. Input vertices (without incoming edges) labelled with **0**, **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 **1**?

Theorem (Cook-Levin)

CSAT *is* **NP-Complete**.

Need to show

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

Monotone CSAT?

Consider an instance of **CSAT** of size n, that does not contain any negations. This problem **Monotone CSAT** is

(A) **NP-Hard**.

(B) **NP-Complete**.

(C) **P**.

(D) Solvable in linear time.

(E) Solvable in $O(2^n)$ time.

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: 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.

Converting into circuit...

Assume any polynomial time algorithm can be converted into a boolean circuit in polynomial time. Then

(A) A certifier $\mathbf{C(s,t)}$ is a polynomial algorithm, and as such there a boolean circuit of polynomial size that implements it.

(B) A certifier $\mathbf{C(s,t)}$ can not be implemented as a circuit since $\mathbf{t}$ (the certificate) is not known.

(C) There are some certifiers (but not all) that can be implemented as a boolean circuit.

(D) Only certifiers for problems in **P** are convertible into circuits.

CSAT is NP-hard: Idea

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

What does it mean that $\mathbf{X} \in \mathbf{NP}$?
$\mathbf{X} \in \mathbf{NP}$ implies that there are polynomials $\mathbf{p()}$ and $\mathbf{q()}$ and certifier/verifier program **C** such that for every string **s** the following is true:

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

Reducing $\mathbf{X}$ to $\mathbf{CSAT}$

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

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

Reducing X to CSAT

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

Problem X: Given string **s**, is $\mathbf{s} \in \mathbf{X}$?

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

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

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

Reducing X to CSAT

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

Problem X: Given string **s**, is $\mathbf{s} \in \mathbf{X}$?

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

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

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

Reducing X to CSAT

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

Problem X: Given string **s**, is $\mathbf{s} \in \mathbf{X}$?

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

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

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

Reducing X to CSAT

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

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

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

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

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

Reducing X to CSAT

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

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

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

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

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

Reducing X to CSAT

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

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

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

1. Convert $\mathbf{C}(\mathbf{s}, \mathbf{t})$ into a circuit $\mathbf{G}$ with $\mathbf{t}$ as unknown inputs (rest is known including $\mathbf{s}$)
2. We know that $|\mathbf{t}| = \mathbf{p}(|\mathbf{s}|)$ so express boolean string $\mathbf{t}$ as $\mathbf{p}(|\mathbf{s}|)$ variables $\mathbf{t}_1, \mathbf{t}_2, \ldots, \mathbf{t}_k$ where $\mathbf{k} = \mathbf{p}(|\mathbf{s}|)$.
3. Asking if there is a proof $\mathbf{t}$ that makes $\mathbf{C}(\mathbf{s}, \mathbf{t})$ say YES is same as whether there is an assignment of values to "unknown" variables $\mathbf{t}_1, \mathbf{t}_2, \ldots, \mathbf{t}_k$ that will make $\mathbf{G}$ evaluate to true/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.

Reducing X to CSAT

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

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

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

1. Convert $\mathbf{C}(\mathbf{s}, \mathbf{t})$ into a circuit $\mathbf{G}$ with $\mathbf{t}$ as unknown inputs (rest is known including $\mathbf{s}$)
2. We know that $|\mathbf{t}| = \mathbf{p}(|\mathbf{s}|)$ so express boolean string $\mathbf{t}$ as $\mathbf{p}(|\mathbf{s}|)$ variables $\mathbf{t}_1, \mathbf{t}_2, \ldots, \mathbf{t}_k$ where $\mathbf{k} = \mathbf{p}(|\mathbf{s}|)$.
3. Asking if there is a proof $\mathbf{t}$ that makes $\mathbf{C}(\mathbf{s}, \mathbf{t})$ say YES is same as whether there is an assignment of values to "unknown" variables $\mathbf{t}_1, \mathbf{t}_2, \ldots, \mathbf{t}_k$ that will make $\mathbf{G}$ evaluate to true/YES.

Reducing X to CSAT

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

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

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

1. Convert $\mathbf{C}(\mathbf{s}, \mathbf{t})$ into a circuit $\mathbf{G}$ with $\mathbf{t}$ as unknown inputs (rest is known including $\mathbf{s}$)
2. We know that $|\mathbf{t}| = \mathbf{p}(|\mathbf{s}|)$ so express boolean string $\mathbf{t}$ as $\mathbf{p}(|\mathbf{s}|)$ variables $\mathbf{t}_1, \mathbf{t}_2, \ldots, \mathbf{t}_k$ where $\mathbf{k} = \mathbf{p}(|\mathbf{s}|)$.
3. Asking if there is a proof $\mathbf{t}$ that makes $\mathbf{C}(\mathbf{s}, \mathbf{t})$ say YES is same as whether there is an assignment of values to "unknown" variables $\mathbf{t}_1, \mathbf{t}_2, \ldots, \mathbf{t}_k$ that will make $\mathbf{G}$ evaluate to true/YES.

Reducing X to CSAT

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

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

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

1. Convert $\mathbf{C}(\mathbf{s}, \mathbf{t})$ into a circuit $\mathbf{G}$ with $\mathbf{t}$ as unknown inputs (rest is known including $\mathbf{s}$)
2. We know that $|\mathbf{t}| = \mathbf{p}(|\mathbf{s}|)$ so express boolean string $\mathbf{t}$ as $\mathbf{p}(|\mathbf{s}|)$ variables $\mathbf{t}_1, \mathbf{t}_2, \ldots, \mathbf{t}_k$ where $\mathbf{k} = \mathbf{p}(|\mathbf{s}|)$.
3. Asking if there is a proof $\mathbf{t}$ that makes $\mathbf{C}(\mathbf{s}, \mathbf{t})$ say YES is same as whether there is an assignment of values to "unknown" variables $\mathbf{t}_1, \mathbf{t}_2, \ldots, \mathbf{t}_k$ that will make $\mathbf{G}$ evaluate to true/YES.

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.

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

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.

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

Example: Independent Set

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

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

Certifier for Independent Set

Certifier $\mathbf{C(s,t)}$ 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
```

$$
\begin{array}{l}
\textbf{if } (t_1 + t_2 + \ldots + t_n < k) \textbf{ then} \\
\quad \textbf{return } \texttt{NO} \\
\textbf{else} \\
\quad \textbf{for } \texttt{each } (i,j) \textbf{ do} \\
\quad\quad \textbf{if } (t_i \wedge t_j \wedge y_{i,j}) \textbf{ then} \\
\quad\quad\quad \textbf{return } \texttt{NO} \\
\\
\textbf{return } \texttt{YES}
\end{array}
$$

Example: Independent Set

A certifier circuit for Independent Set

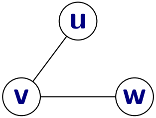
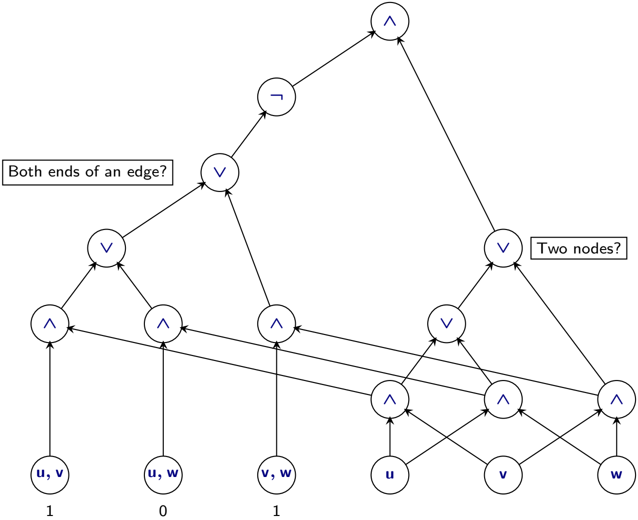


Figure : Graph **G** with $\mathbf{k = 2}$



What does the following formula compute?

The formula

$$\mathbf{F}(\mathbf{x}_1, \ldots, \mathbf{x}_n) = \bigwedge_{i<j} (\overline{\mathbf{x}_i} \vee \overline{\mathbf{x}_j}) \,.$$

is true if and only if

(A) All the $\mathbf{x}_i$s are one.

(B) All the $\mathbf{x}_i$s are zero.

(C) There are exactly two ones in $\mathbf{x}_1, \ldots, \mathbf{x}_n$.

(D) There is at most one bit one in $\mathbf{x}_1, \ldots, \mathbf{x}_n$.

(E) There are at most two ones in $\mathbf{x}_1, \ldots, \mathbf{x}_n$.

What does the following formula compute?

The formula

$$\mathbf{H}(\mathbf{x}_1, \ldots, \mathbf{x}_n) = \left(\bigwedge_{i<j} (\overline{\mathbf{x}_i} \vee \overline{\mathbf{x}_j}) \right) \wedge (\mathbf{x}_1 \vee \mathbf{x}_2 \vee \cdots \mathbf{x}_n).$$

is true if and only if

(A) All the $\mathbf{x}_i$s are one.

(B) There are exactly two ones in $\mathbf{x}_1, \ldots, \mathbf{x}_n$.

(C) There is exactly one bit one in $\mathbf{x}_1, \ldots, \mathbf{x}_n$.

(D) There is at most one bit one in $\mathbf{x}_1, \ldots, \mathbf{x}_n$.

(E) There are at most two ones in $\mathbf{x}_1, \ldots, \mathbf{x}_n$.

What does the following formula compute?

$\langle \mathbf{G} \rangle$: a vector of $\binom{n}{2}$ bits describing a graph with $\mathbf{n}$ vertices.
$\mathbf{I}(\mathbf{x}_1, \ldots, \mathbf{x}_n, \langle \mathbf{G} \rangle)$ formula true $\Leftrightarrow$ $\mathbf{x}_1, \ldots, \mathbf{x}_n$ independent set in $\mathbf{G}$.
Input: $\left\langle \mathbf{x}_1^1, \mathbf{x}_1^2, \mathbf{x}_1^3, \quad \mathbf{x}_2^1, \mathbf{x}_2^2, \mathbf{x}_2^3, \quad \ldots, \quad \mathbf{x}_n^1, \mathbf{x}_n^2, \mathbf{x}_n^3, \quad \mathbf{G} \right\rangle$.
The formula

$$\left(\bigwedge_{i=1}^{n} \mathbf{H}\left(\mathbf{x}_i^1, \mathbf{x}_i^2, \mathbf{x}_i^3\right) \right) \bigwedge \mathbf{I}\left(\mathbf{x}_1^1, \mathbf{x}_2^1, \mathbf{x}_3^1, \ldots, \mathbf{x}_n^1, \langle \mathbf{G} \rangle\right)$$
$$\bigwedge \mathbf{I}\left(\mathbf{x}_1^2, \mathbf{x}_2^2, \mathbf{x}_3^2, \ldots, \mathbf{x}_n^2, \langle \mathbf{G} \rangle\right) \bigwedge \mathbf{I}\left(\mathbf{x}_1^3, \mathbf{x}_2^3, \mathbf{x}_3^3, \ldots, \mathbf{x}_n^1, \langle \mathbf{G} \rangle\right)$$

is satisfiable if and only if

- **(A)** The graph $\mathbf{G}$ contains a clique.
- **(B)** The graph $\mathbf{G}$ can be colored by two colors.
- **(C)** The graph $\mathbf{G}$ can be colored by three colors.
- **(D)** The graph $\mathbf{G}$ encodes a satisfiable instance of 3DM.
- **(E)** None of the above.

Programs, Turing Machines and Circuits

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

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)

Programs, Turing Machines and Circuits

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

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 are TMs

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

Problem: Given $\mathbf{M}$, input $\mathbf{s}$, $\mathbf{p}$, $\mathbf{q}$ decide if there is a proof $\mathbf{t}$ of length $\mathbf{p}(|\mathbf{s}|)$ such that $\mathbf{M}$ on $\mathbf{s}, \mathbf{t}$ will halt in $\mathbf{q}(|\mathbf{s}|)$ 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 $\mathbf{p}(|\mathbf{s}|)$ and $\mathbf{q}(|\mathbf{s}|)$.
2. Knows that $\mathbf{M}$ can use at most $\mathbf{q}(|\mathbf{s}|)$ memory/tape cells
3. Knows that $\mathbf{M}$ can run for at most $\mathbf{q}(|\mathbf{s}|)$ time
4. Simulates the evolution of the state of $\mathbf{M}$ and memory over time using a big circuit.

Simulation of Computation via Circuit

1. Think of $\mathbf{M}$'s state at time ℓ as a string $\mathbf{x}^\ell = \mathbf{x}_1\mathbf{x}_2\ldots\mathbf{x}_k$ where each $\mathbf{x}_i \in \{0, 1, B\} \times Q \cup \{q_{-1}\}$.
2. At time $\mathbf{0}$ the state of $\mathbf{M}$ consists of input string $\mathbf{s}$ a guess $\mathbf{t}$ (unknown variables) of length $\mathbf{p}(|\mathbf{s}|)$ and rest $\mathbf{q}(|\mathbf{s}|)$ blank symbols.
3. At time $\mathbf{q}(|\mathbf{s}|)$ we wish to know if $\mathbf{M}$ stops in $\mathbf{q}_{\mathbf{accept}}$ with say all blanks on the tape.
4. We write a circuit $\mathbf{C}_\ell$ which captures the transition of $\mathbf{M}$ from time ℓ to time $\ell + 1$.
5. Composition of the circuits for all times $\mathbf{0}$ to $\mathbf{q}(|\mathbf{s}|)$ 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 $\mathbf{M}$ 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.

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.

To show **NP-Complete**ness

Let **X** be a decision problem.
We know that **CSAT** is **NP-Complete**.
To show that **X** is **NP-Complete** we need to:

(A) Provide a polynomial time reduction from **X** to **CSAT**.

(B) Provide a polynomial time reduction from **X** to **CSAT** and show that $\mathbf{X} \in \mathbf{NP}$.

(C) Provide a polynomial time reduction from **CSAT** to **X**.

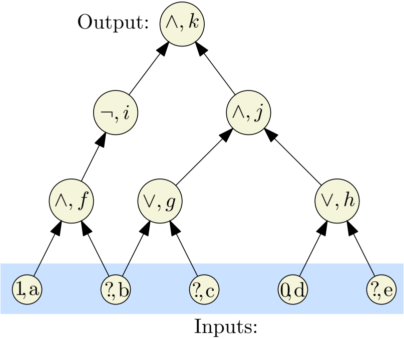
(D) Provide a polynomial time reduction from **CSAT** to **X** and show that $\mathbf{X} \in \mathbf{NP}$.

(E) Provide a polynomial time reduction from **CSAT** to **X** and show that $\mathbf{X} \notin \mathbf{P}$.

SAT is NP-Complete

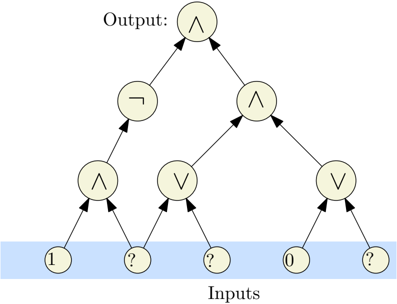
1. We have seen that **SAT** $\in$ **NP**
2. To show **NP-Hardness**, we will reduce Circuit Satisfiability (**CSAT**) to **SAT**

   Instance of **CSAT** (we label each node):

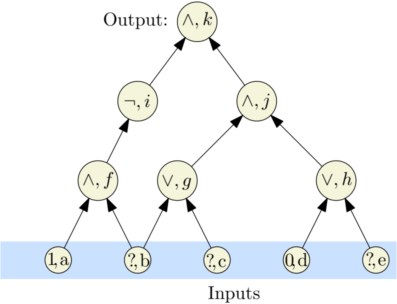


Converting a circuit into a CNF formula

Label the nodes



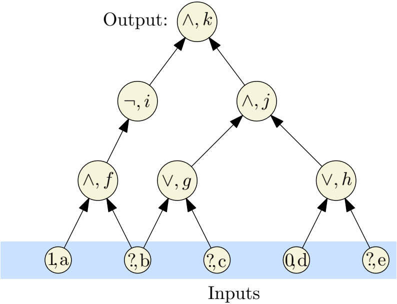
(A) Input circuit



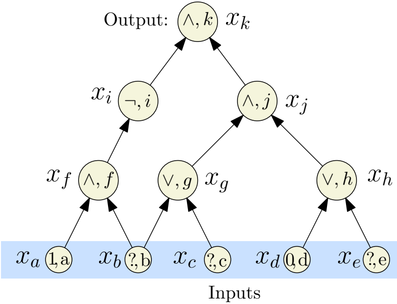
(B) Label the nodes.

Converting a circuit into a CNF formula

Introduce a variable for each node



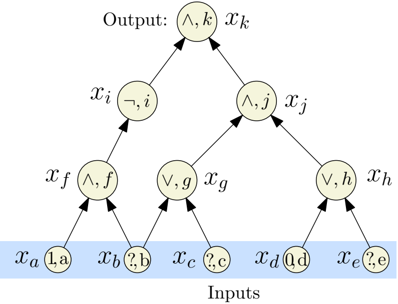
(B) Label the nodes.



(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.



$\mathbf{x_k}$ (Demand a sat' assignment!)

$\mathbf{x_k = x_i \wedge x_k}$

$\mathbf{x_j = x_g \wedge x_h}$

$\mathbf{x_i = \neg x_f}$

$\mathbf{x_h = x_d \vee x_e}$

$\mathbf{x_g = x_b \vee x_c}$

$\mathbf{x_f = x_a \wedge x_b}$

$\mathbf{x_d = 0}$

$\mathbf{x_a = 1}$

(C) Introduce var for each node.

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

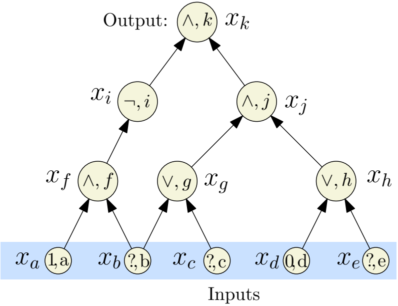
Converting a circuit into a CNF formula

Convert each sub-formula to an equivalent CNF formula

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

Converting a circuit into a CNF formula

Take the conjunction of all the CNF sub-formulas



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

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

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

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

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

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 $\mathbf{C}$ is satisfiable iff $\varphi_{\mathbf{C}}$ is satisfiable

$\Rightarrow$ Consider a satisfying assignment $\mathbf{a}$ for $\mathbf{C}$

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

$\Leftarrow$ Consider a satisfying assignment $\mathbf{a}$ for $\varphi_{\mathbf{C}}$

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

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 $\mathbf{C(s, t)}$
2. Reduction from a known **NP-Complete** problem such as **CSAT** or **SAT** to **X**

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

$\mathbf{Y} \leq_P \mathbf{SAT}$ and $\mathbf{SAT} \leq_P \mathbf{X}$ and hence $\mathbf{Y} \leq_P \mathbf{X}$.

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 $\mathbf{C(s,t)}$
2. Reduction from a known **NP-Complete** problem such as **CSAT** or **SAT** to **X**

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

$\mathbf{Y} \leq_P \mathbf{SAT}$ and $\mathbf{SAT} \leq_P \mathbf{X}$ and hence $\mathbf{Y} \leq_P \mathbf{X}$.

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 $\mathbf{C(s, t)}$
2. Reduction from a known **NP-Complete** problem such as **CSAT** or **SAT** to **X**

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

$\mathbf{Y} \leq_P \mathbf{SAT}$ and $\mathbf{SAT} \leq_P \mathbf{X}$ and hence $\mathbf{Y} \leq_P \mathbf{X}$.

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!

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!

Notes

Notes

Notes

Notes