Polynomial reducibility. The class NP

Recall: TM Configurations

A configuration of a TM with k tapes, the tape symbol set Γ, and state set Q is

$$\langle q; w_1, \ldots, w_k; p_1, \ldots, p_k \rangle, \text{ where}$$

- $q \in Q$ is the current state of the TM;
- $w_i \in \Gamma^* \cdot \{\Box^\omega\}$ is the contents of the i-th tape.
  - w_i consists of a finite sequence of elements of Γ, followed by infinitely many $\Box$-s.
- $p_i \in \mathbb{N}$ is the position of the i-th head. Let leftmost position be 1.

Let $\mathcal{CONF}^k_{\Gamma,Q}$ be the set of all such configurations.

Recall: TM computations

A TM $M = (\Gamma, Q, \delta, q_0, Q_F)$ defines a relation (actually, a partial function) $\xrightarrow{M}$ on $\mathcal{CONF}^k_{\Gamma,Q}$.

$$\langle q; w_1, \ldots, w_k; p_1, \ldots, p_k\rangle \xrightarrow{M} \langle q'; w_1, w'_2, \ldots, w'_k; p'_1, \ldots, p'_k\rangle \text{ iff}$$

- $q \notin Q_F$
- $\gamma_i = w_i[p_i]$
- $(q'; \gamma'_2, \ldots, \gamma'_k; s_1, \ldots, s_k) = \delta(q; \gamma_1, \ldots, \gamma_k)$
- $w'_i = w_i[p_i \mapsto \gamma'_i]$
- $p'_i = \max(1, p_i + s_i)$

Configurations and computation steps as a graph

Given M with k tapes, tape alphabet Γ and set of states Q, we may consider a directed graph:

- Set of vertices is the set of configurations $\mathcal{CONF}^k_{\Gamma,Q}$.
- An edge goes from configuration C to configuration C' iff $C \stackrel{M}{\to} C'$.

Properties

- Any configuration C has at most one outgoing edge.
- If M accepts a language L in time T, then for any $x \in \{0,1\}^*$, the path starting in the starting configuration corresponding to x has length bounded by $T(|x|)$.

Nondeterministic Turing Machines

- deterministic transition function:

$$\delta : Q \times \Gamma^k \to Q \times \Gamma^{k-1} \times \mathsf{Move}^k$$

- nondeterministic transition relation

$$\delta \subseteq \left(Q \times \Gamma^k\right) \times \left(Q \times \Gamma^{k-1} \times \mathsf{Move}^k\right)$$

- (all other components of a TM remain the same)

In the computation graph, a configuration may have more than one outgoing edge.

NTM accepting a language

An NTM M accepts a language $L \subseteq \{0,1\}^*$ in time T if for all $x \in L$, there exists a path of length at most $T(|x|)$ in the computation graph of M from the starting configuration for x to some accepting configuration.

- What about the length of other paths from this starting configuration?
- What about the length of paths from starting configuration for some $y \notin L$?

We choose to not put any restrictions on them.

Exercise. Show that if an NTM M accepts the language L in time T, then exists NTM M' that accepts L and where all path from starting configurations have length at most $O(T)$.

Non-deterministic RAM

- Has nondeterministic choice operation $T \leftarrow \{0, 1\}$.
  - The value of the register T will be nondeterministically chosen as 0 or 1.
  - The configuration of RAM where this instruction is executed will have two successors in the RAM's computation graph.

NRAM-s and NTM-s can simulate each other without much loss in efficiency.

classes NTIME and NP

- Let $f : \mathbb{N} \to \mathbb{N}$
- The class $\mathsf{NTIME}(f) \subseteq 2^{\{0,1\}^*}$ is the set of all languages L, where
  - exists $g : \mathbb{N} \to \mathbb{N}$, such that
  - exists NTM M that accepts L in time g, and
  - $g \in O(f)$.

$$\mathsf{NP} = \bigcup_{c \in \mathbb{N}} \mathsf{NTIME}(\lambda n.n^c)$$

If we replaced “NTM” with “NRAM”, the class NP would stay the same.

NP as a class of verification problems

Theorem. $L \in$ NP iff

- there exists a DTM M and a polynomial p, such that
  - $x \in L$

  iff

  - $\exists y \in \{0,1\}^*$ with $|y| \leq p(|x|)$, such that
  - $M(x, y)$ accepts in at most $p(|x|)$ steps.

y may be seen as the certificate that $x \in L$.

Examples

Many searching problems.

- Does a graph G have a clique of size at least k?
- Does a boolean formula with variables have a satisfying assignment to those variables?
- Does a weighted graph have a traveling salesman tour of length at most k?
- Is a number n composite?
- Can the vertices of a graph be colored with three colors?
- Are two graphs (given e.g. by their adjacency lists) isomorphic?
- Do the vertices u and v of some graph belong to the same connected component?

Relation between P and NP

Theorem. P $\subseteq$ NP $\subseteq \bigcup_{c\in\mathbb{N}}$ DTIME(2^{n^c}).

- Left inclusion: every DTM is a NTM.
- Right inclusion: using time $2^{O(p(n))}$ we can check every certificate of length $p(n)$.

Right inclusion in more general form:
Theorem. NTIME$(f) \subseteq \bigcup_{c\in\mathbb{N}}$ DTIME$(\lambda n.c^{f(n)})$.

Polynomial reducibility

A language L is polynomially [many-one] reducible to a language L' if

- exists a polynomial-time computable function $f : \{0,1\}^* \to \{0,1\}^*$, such that
- for all $x \in \{0,1\}^*$
- $x \in L$ iff $f(x) \in L'$.

Denote $L \leq_{\mathrm{m}}^{\mathrm{P}} L'$.

- we think f as "easily" computable.
- Hence, if we know how to test membership in L', we also know how to test membership in L.
- We can say that membership problem for L' is at least as hard as membership problem for L.

Properties of polynomial reducibility.

- If $L_1 \leq_{\mathrm{m}}^{\mathrm{P}} L_2$ and $L_2 \leq_{\mathrm{m}}^{\mathrm{P}} L_3$ then $L_1 \leq_{\mathrm{m}}^{\mathrm{P}} L_3$
- If $L_1 \leq_{\mathrm{m}}^{\mathrm{P}} L_2$ and $L_2 \in \mathsf{P}$ then $L_1 \in \mathsf{P}$
- If $L_1 \leq_{\mathrm{m}}^{\mathrm{P}} L_2$ and $L_2 \in \mathsf{NP}$ then $L_1 \in \mathsf{NP}$

For a language $L \subseteq \{0,1\}^*$ denote $L^{\mathrm{c}} = \{0,1\}^* \backslash L$.

- If $L_1 \leq_{\mathrm{m}}^{\mathrm{P}} L_2$ then ${L_1}^{\mathrm{c}} \leq_{\mathrm{m}}^{\mathrm{P}} {L_2}^{\mathrm{c}}$.

NP-**hardness and** NP-**completeness**

- A language L is NP-hard if for all $L' \in \mathrm{NP}$ we have $L' \leq_{\mathrm{m}}^{\mathrm{P}} L$.
- A language L is NP-complete if L is NP-hard and $L \in \mathrm{NP}$.

- If a language L is NP-hard and $L \in \mathrm{P}$ then $\mathrm{P} = \mathrm{NP}$.
- If a language L is NP-complete then $L \in \mathrm{P}$ if and only if $\mathrm{P} = \mathrm{NP}$.

Existence of NP-complete languages

Theorem. There exist NP-complete languages.

Proof. Consider the following language. We show that it is NP-complete.

$$L = \{\langle M, x, 1^n \rangle \,|\, \text{NTM } M \text{ accepts } x \text{ in at most } n \text{ steps}\}$$

L is in NP. The certificate consists of the choices M must make to accept x.

L is NP-hard.

- Let $L' \in$ NP. Let M' be a NTM that accepts L' in time T.
- Let $f(x) = \langle M', x, 1^{T(|x|)} \rangle$. This f shows that $L' \leq_{\mathrm{m}}^{\mathrm{P}} L$.

SAT

- A boolean formula over variables $u_1, \ldots, u_n$ consists of those variables and the logical operators $\vee$, $\wedge$, $\neg$,… connecting them.
  - Let $\mathcal{BF}$ be the set of all boolean formulas.
- A valuation of $u_1, \ldots, u_n$ is a mapping from $\{u_1, \ldots, u_n\}$ to $\{\mathsf{true}, \mathsf{false}\}$.
- A boolean formula evaluates to true for no, some, or all valuations of $u_1, \ldots, u_n$.
  - $u_1 \wedge \neg u_1$ is unsatisfiable;
  - $(u_1 \wedge u_2) \vee (u_2 \wedge \neg u_3)$ is satisfiable;
  - $((u_1 \rightarrow u_2) \rightarrow u_1) \rightarrow u_1$ is tautology.
- SAT is the language $\{\varphi \in \mathcal{BF} \mid \varphi \text{ is satisfiable}\}$.

CNFSAT and k-CNFSAT

- A literal is either a boolean variable or its negation.
- A disjunct is $l_1 \vee l_2 \vee \cdots \vee l_r$, where $l_1, \ldots, l_r$ are literals.
- A boolean formula is in conjuctive normal form if it is of the form $D_1 \wedge D_2 \wedge \cdots \wedge D_m$, where $D_1, \ldots, D_m$ are disjuncts.
  - Let $\mathcal{CNF}$ be the language of all boolean formulas in conjuctive normal form.
  - Let k-$\mathcal{CNF}$ be the language of all boolean formulas in conjuctive normal form, where no disjunct has more than k literals.
- CNFSAT is the language $\{\varphi \in \mathcal{CNF} \mid \varphi \text{ is satisfiable}\}$.
- k-CNFSAT is the language $\{\varphi \in k\text{-}\mathcal{CNF} \mid \varphi \text{ is satisfiable}\}$.

Reducibility of SAT and CNFSAT

Theorem. If $k \geq 3$ then SAT $\leq_{\mathrm{m}}^{\mathrm{P}}$ k-CNFSAT $\leq_{\mathrm{m}}^{\mathrm{P}}$ CNFSAT $\leq_{\mathrm{m}}^{\mathrm{P}}$ SAT.

We show SAT $\leq_{\mathrm{m}}^{\mathrm{P}}$ 3-CNFSAT, the rest is trivial.

SAT **is** NP-**complete**

Theorem. SAT is NP-complete.

This result used to be known as Cook's theorem. Now it is more commonly known as Cook-Levin theorem.

- Stephen Cook. The complexity of theorem proving procedures. Proceedings of the Third Annual ACM Symposium on Theory of Computing (STOC). pp. 151–158, 1971.

- Leonid Levin. Universal'nye zadachi perebora. Problemy Peredachi Informatsii **9**(3):265–266, 1973.

Proof. SAT $\in$ NP is trivial.

Succinctly given graphs and SAT

- Let $u_1, \dots, u_n$ be boolean variables. A directed graph can be defined as follows:
  - The vertices of the graph are the valuations of $u_1, \dots, u_n$ satisfying a boolean formula $S(u_1, \dots, u_n)$.
  - The edges are given by a boolean formula $R(u_1, \dots, u_n, u'_1, \dots, u'_n)$.
    - There is an edge from U to V if $R(U(u_1), \dots, U(u_n), V(u_1), \dots, V(u_n))$ is true.

  Such R is a succinct representation of some graph.

- Let two sets of vertices be given by two formulas Φ°, $\Phi^\bullet$.

- We show how to write a formula $\mathrm{Path}^k_R[\Phi^\circ, \Phi^\bullet]$ that is satisfiable iff there is a path of length at most k from some vertex in Φ° to some vertex in $\Phi^\bullet$. Assumption of seriality: there is an edge out of each vertex.

$\mathrm{Path}^k_R[\Phi^\circ, \Phi^\bullet]$

Use the variables $u_1^0, \dots, u_n^0, u_1^1, \dots, u_n^1, \dots, u_1^k, \dots, u_n^k$. Form the conjunction of

- $S(u_1^0, \dots, u_n^0)$
- $S(u_1^1, \dots, u_n^1)$
- $\dots$
- $S(u_1^k, \dots, u_n^k)$

- $R(u_1^0, \dots, u_n^0, u_1^1, \dots, u_n^1)$
- $R(u_1^1, \dots, u_n^1, u_1^2, \dots, u_n^2)$
- $\dots$
- $R(u_1^{k-1}, \dots, u_n^{k-1}, u_1^k, \dots, u_n^k)$

- $\Phi^\circ(u_1^0, \dots, u_n^0)$
- $\bigvee_{i=0}^k \Phi^\bullet(u_1^i, \dots, u_n^i)$

The size of $\mathrm{Path}^k_R[\Phi^\circ, \Phi^\bullet]$ is polynomial in $|S|$, $|R|$, k.

Meaning of $\mathrm{Path}_R^k[\Phi^\circ, \Phi^\bullet]$

- Consider a valuation satisfying $\mathrm{Path}_R^k[\Phi^\circ, \Phi^\bullet]$.
- It defines a sequence of $k+1$ vertices (satisfying S).
- First vertex in Φ°. Some vertex in $\Phi^\bullet$.
- Edge from each vertex to the next one.

Vice versa, if there is a path from $\Phi^c irc$ to $\Phi^\bullet$ with length $\leq k$, then

- Any extension of this path to length k will satisfy $\mathrm{Path}_R^k[\Phi^\circ, \Phi^\bullet]$.

Succinct representation of computation graphs

- Consider a k-tape NTM $M = (\Gamma, Q, \delta, q_0, \{q_{\mathsf{acc}}, q_{\mathsf{rej}}\})$ working in time T.
- Let x be its input.
- Consider the subset $\mathcal{C}$ of $\mathcal{CONF}^k_{\Gamma,Q}$ of configurations of size at most $T(|x|)$.

We can represent the elements of $\mathcal{C}$ as valuations of a certain set of boolean variables.

(The variables, the formulas S and R and their sizes will be discussed on the blackboard)