Computational Complexity Theory

Lecture 7: Class EXP; Time Hierarchy Theorem

Department of Computer Science,
Indian Institute of Science

Recap: Nondeterministic Turing Machines

- A *nondeterministic Turing machine* is like a deterministic Turing machines but with two transition functions.
- It is formally defined by a tuple $(\Gamma, Q, \delta_0, \delta_1)$. It has a special state q_{accept} in addition to q_{start} and q_{halt}.
- At every step of computation, the machine applies one of two functions δ_0 and δ_1 *arbitrarily*.
- Unlike DTMs, NTMs are **not intended to be physically realizable** (because of the arbitrary nature of application of the transition functions).

Recap: Nondeterministic Turing Machines

- Definition. An NTM M *accepts* a string $x \in \{0,1\}^*$ iff on input x there ***exists*** a sequence of applications of the transition functions δ_0 and δ_1 (beginning from the start configuration) that makes M reach q_{accept}.

- Defintion. An NTM M *decides* L in $T(|x|)$ time if
  - M accepts x $\longleftrightarrow$ $x \in L$
  - On <u>every sequence</u> of applications of the transition functions on input x, M either reaches q_{accept} or q_{halt} within $T(|x|)$ steps of computation.

Recap: Alternate characterization of NP

- Definition. A language L is in $NTIME(T(n))$ if there's an NTM M that decides L in $c.\,T(n)$ time on inputs of length n, where c is a constant.

- Theorem. $NP = \bigcup_{c>0} NTIME(n^c)$.

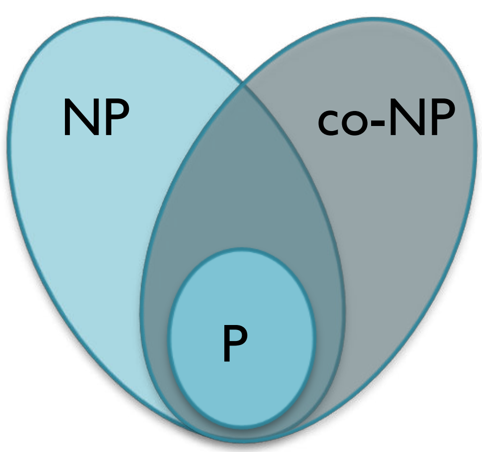
  Proof sketch: Let L be a language in NP. Then, there's a poly-time verifier M s.t,

$$x \in L \iff \exists u \in \{0,1\}^{p(|x|)} \text{ s.t. } M(x,u) = 1$$

Recap: Class co-NP

- Definition. For every $L \subseteq \{0,1\}^*$ let $\overline{L} = \{0,1\}^* \setminus L$.
  A language L is in co-NP if $\overline{L}$ is in NP.

- Example. $\overline{\text{SAT}} = \{\phi : \phi$ is *not* satisfiable$\}$.



Recap: Class co-NP : Alternate definition

- Recall, a language $L \subseteq \{0,1\}^*$ is in NP if there's a *poly function* p and a *poly-time verifier* M such that

$$x \in L \Leftrightarrow \exists u \in \{0,1\}^{p(|x|)} \text{ s.t. } M(x,u) = 1$$

$$x \in \bar{L} \Leftrightarrow \forall u \in \{0,1\}^{p(|x|)} \text{ s.t. } M(x,u) = 0$$

$$x \in \bar{L} \Leftrightarrow \forall u \in \{0,1\}^{p(|x|)} \text{ s.t. } \bar{M}(x,u) = 1$$

- Definition. A language $L \subseteq \{0,1\}^*$ is in co-NP if there's a *poly function* p and a *poly-time TM* M such that

$$x \in L \Leftrightarrow \forall u \in \{0,1\}^{p(|x|)} \text{ s.t. } M(x,u) = 1$$

for NP this was $\exists$

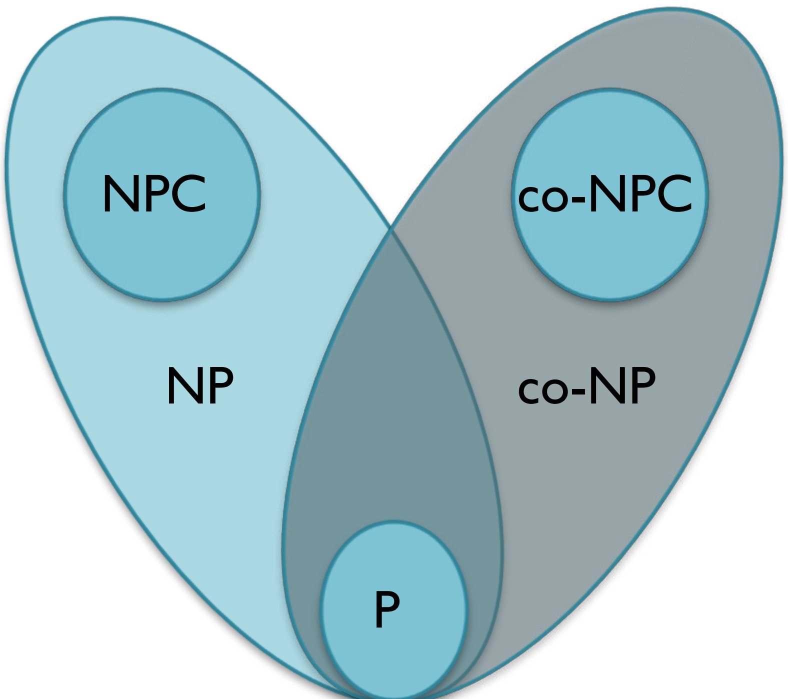
Recap: co-NP-completeness

- Definition. A language $L' \subseteq \{0,1\}^*$ is co-NP-complete if
  - ➢ L' is in co-NP
  - ➢ Every language L in co-NP is polynomial-time (Karp) reducible to L'.

- Theorem. $\overline{\text{SAT}}$ and TAUTOLOGY are co-NP-complete.

- Theorem. If L in NP-complete then L is co-NP-complete

The diagram again



If a co-NP complete language belongs to NP then

co-NP $\subseteq$ NP

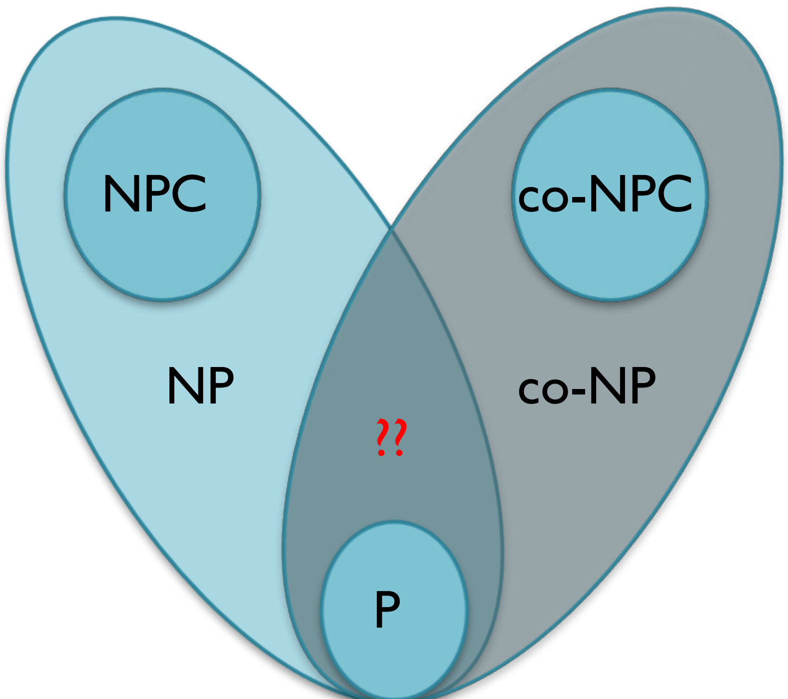
$\Rightarrow$ co-NP = NP

Let C_1 and C_2 be two complexity classes.

If $C_1 \subseteq C_2$, then co-$C_1 \subseteq$ co-C_2.

Obs. co-(co-C) = C .

The diagram again



If a co-NP-complete language belongs to NP then

co-NP $\subseteq$ NP

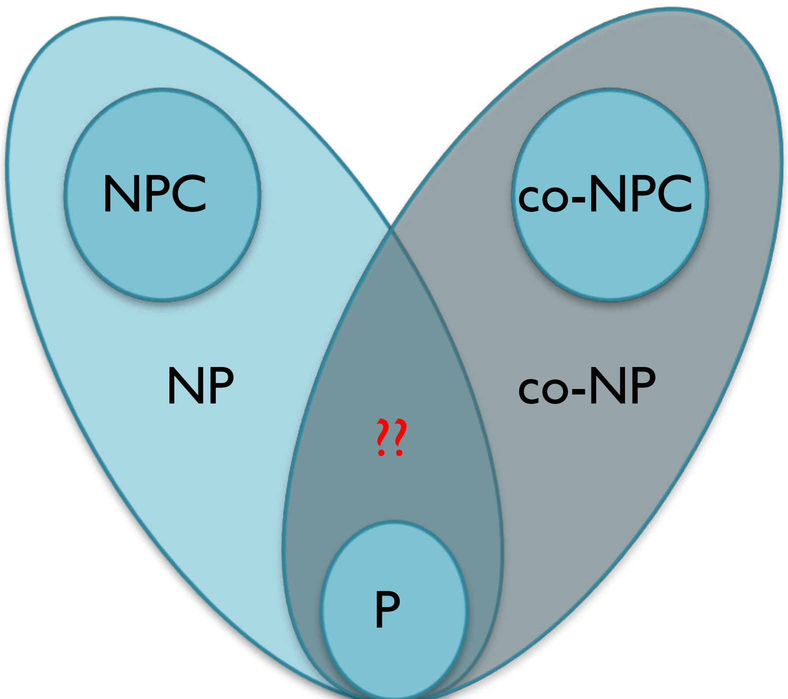
→ co-NP = NP

Let C_1 and C_2 be two complexity classes.

If $C_1 \subseteq C_2$, then co-$C_1 \subseteq$ co-C_2.

Obs. co-(co-C) = C .

The diagram again



If an NP-complete language belongs to co-NP then

$\Rightarrow$ NP $\subseteq$ co-NP
NP = co-NP

Let C_1 and C_2 be two complexity classes.

If $C_1 \subseteq C_2$, then co-$C_1 \subseteq$ co-C_2.

Obs. co-(co-C) = C .

Integer factoring in NP ∩ co-NP

- Integer factoring.

  FACT = {(N, U): there's a prime in [U] dividing N}

- Claim. FACT ∈ NP ∩ co-NP

- So, FACT is NP-complete implies NP = co-NP.

Integer factoring in NP ∩ co-NP

- Integer factoring.

  FACT = {(N, U): there's a prime in [U] dividing N}

- Claim. FACT ∈ NP ∩ co-NP
- Proof. FACT ∈ NP : Give p as a certificate. The verifier checks if p is prime (AKS test), $1 \leq p \leq U$ and p divides N.

Integer factoring in NP ∩ co-NP

- Integer factoring.

  FACT = {(N, U): there's a prime in [U] dividing N}

- Claim. FACT ∈ NP ∩ co-NP
- Proof. FACT ∈ NP : Give the complete prime factorization of N as a certificate. The verifier checks the correctness of the factorization, and then checks if none of the prime factors is in [U].

Integer factoring in NP ∩ co-NP

- Integer factoring.

  FACT = {(N, U): there's a prime in [U] dividing N}

- Claim. FACT ∈ NP ∩ co-NP
- Proof. FACT ∈ NP : Give the complete prime factorization of N as a certificate. The verifier checks the correctness of the factorization, and then checks if none of the prime factors is in [U].

- Homework: If FACT ∈ P, then there's a algorithm to find the prime factorization a given n-bit integers in poly(n) time.

Integer factoring in NP ∩ co-NP

- Integer factoring.

  FACT = {(N, U): there's a prime in [U] dividing N}

- Factoring algorithm. Dixon's randomized algorithm factors an n-bit number in $\exp(O(\sqrt{n} \log n))$ time.

Class EXP

- Definition. Class EXP is the exponential time analogue of class P.

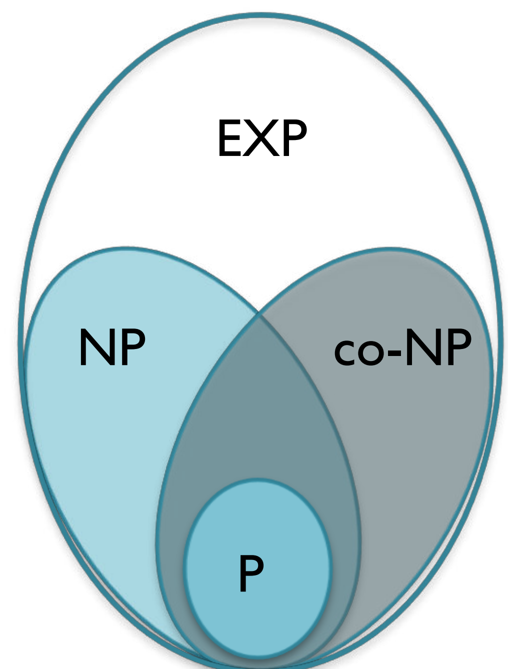
$$EXP = \bigcup_{c \geq 1} DTIME(2^{n^c})$$

Class EXP

- Definition. Class EXP is the exponential time analogue of class P.

$$\text{EXP} = \bigcup_{c \geq 1} \text{DTIME}(2^{n^c})$$

- Observation. $\text{P} \subseteq \boxed{\text{NP} \subseteq \text{EXP}}$



Class EXP

- Definition. Class EXP is the exponential time analogue of class P.

$$EXP = \bigcup_{c \geq 1} DTIME\left(2^{n^c}\right)$$

- Observation. $P \subseteq NP \subseteq EXP$

- *Exponential Time Hypothesis.* *(Impagliazzo & Paturi 1999)* Any algorithm for 3-SAT takes $\geq 2^{\delta . n}$ time, where $\delta > 0$ is some fixed constant and n is the no. of variables.

In other words, δ cannot be made arbitrarily close to 0.

Class EXP

- **Definition.** Class EXP is the exponential time analogue of class P.

$$\mathrm{EXP} = \bigcup_{c \geq 1} \mathrm{DTIME}\left(2^{n^c}\right)$$

- **Observation.** $\mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{EXP}$

- *Exponential Time Hypothesis.* *(Impagliazzo & Paturi 1999)* Any algorithm for 3-SAT takes $\geq 2^{\delta . n}$ time, where $\delta > 0$ is some fixed constant and n is the no. of variables.

$$\mathrm{ETH} \Rightarrow \mathrm{P} \neq \mathrm{NP}$$

Class EXP

- Definition. Class EXP is the exponential time analogue of class P.

$$\mathrm{EXP} = \bigcup_{c \geq 1} \mathrm{DTIME}\left(2^{n^c}\right)$$

- Observation. P $\subseteq$ NP $\subseteq$ EXP

- <u>*Exponential Time Hypothesis.*</u> *(Impagliazzo & Paturi 1999)* Any algorithm for 3-SAT takes $\geq 2^{\delta.n}$ time, where $\delta > 0$ is some fixed constant and n is the no. of variables.

Homework: Read about Strong Exponential Time Hypothesis (SETH).

Diagonalization

Diagonalization

- *Diagonalization* refers to a class of techniques used in complexity theory to separate complexity classes.

Diagonalization

- *Diagonalization* refers to a class of techniques used in complexity theory to separate complexity classes.
- These techniques are characterized by <u>two</u> main features:

Diagonalization

- *Diagonalization* refers to a class of techniques used in complexity theory to separate complexity classes.
- These techniques are characterized by <u>two</u> main features:
    1. There's a universal TM U that when given strings α and x, simulates M_α on x with only a *<u>small</u>* overhead.

Diagonalization

- *Diagonalization* refers to a class of techniques used in complexity theory to separate complexity classes.
- These techniques are characterized by <u>two</u> main features:

  1. There's a universal TM U that when given strings α and x, simulates M_α on x with only a <u>*small*</u> overhead.

     If M_α takes T time on x then U takes $O(T \log T)$ time to simulate M_α on x.

Diagonalization

- *Diagonalization* refers to a class of techniques used in complexity theory to separate complexity classes.
- These techniques are characterized by <u>two</u> main features:
    1. There's a universal TM U that when given strings α and x, simulates M_α on x with only a <u>*small*</u> overhead.

    2. Every string represents some TM, and every TM can be represented by <u>*infinitely many*</u> strings.

Time Hierarchy Theorem

- An application of Diagonalization

Time Hierarchy Theorem

- Let $f(n)$ and $g(n)$ be <u>time-constructible</u> functions s.t.,

  $f(n) \,.\, \log f(n) = o(g(n))$. e.g. $f(n) = n$, $g(n) = n^2$

Time Hierarchy Theorem

- Let $f(n)$ and $g(n)$ be time-constructible functions s.t.,

$$f(n) \,.\, \log f(n) = o(g(n)).$$

- Theorem. $\mathrm{DTIME}(f(n)) \subsetneq \mathrm{DTIME}(g(n))$

Time Hierarchy Theorem

- Let $f(n)$ and $g(n)$ be time-constructible functions s.t.,

$$f(n) \, . \log f(n) = o(g(n)).$$

- Theorem. $\mathrm{DTIME}(f(n)) \subsetneq \mathrm{DTIME}(g(n))$

Proof. We'll prove with $\boxed{f(n) = n \text{ and } g(n) = n^2.}$

Time Hierarchy Theorem

- Let $f(n)$ and $g(n)$ be time-constructible functions s.t.,

  $$f(n) \cdot \log f(n) = o(g(n)).$$

- Theorem. $\mathrm{DTIME}(f(n)) \subsetneq \mathrm{DTIME}(g(n))$

  Proof. We'll prove with $f(n) = n$ and $g(n) = n^2$.

  Task: Show that there's a language L decided by a TM D with time complexity $O(n^2)$ s.t., any TM M with runtime $O(n)$ cannot decide L.

Time Hierarchy Theorem

- Let $f(n)$ and $g(n)$ be time-constructible functions s.t.,

$$f(n) \,.\, \log f(n) = o(g(n)).$$

- Theorem. $\mathrm{DTIME}(f(n)) \subsetneq \mathrm{DTIME}(g(n))$

  Proof. We'll prove with $f(n) = n$ and $g(n) = n^2$.

  TM D :

  1. On input x, compute $|x|^2$.

Time Hierarchy Theorem

- Let $f(n)$ and $g(n)$ be time-constructible functions s.t.,

$$f(n) \,.\, \log f(n) = o(g(n)).$$

- Theorem. $\mathrm{DTIME}(f(n)) \subsetneq \mathrm{DTIME}(g(n))$

  Proof. We'll prove with $f(n) = n$ and $g(n) = n^2$.

  TM D :

  1. On input x, compute $|x|^2$.
  2. Simulate $\boxed{M_x \text{ on } x}$ for $|x|^2$ steps.

D's time steps not M_x's time steps.

Time Hierarchy Theorem

- Let $f(n)$ and $g(n)$ be time-constructible functions s.t.,

$$f(n) \,.\, \log f(n) = o(g(n)).$$

- Theorem. $\mathrm{DTIME}(f(n)) \subsetneq \mathrm{DTIME}(g(n))$

  Proof. We'll prove with $f(n) = n$ and $g(n) = n^2$.

  TM D :

  1. On input x, compute $|x|^2$.
  2. Simulate M_x on x for $|x|^2$ steps.
     a. If M_x stops and outputs b then output $1\text{-}b$.

Time Hierarchy Theorem

- Let $f(n)$ and $g(n)$ be time-constructible functions s.t.,

$$f(n) \,.\, \log f(n) = o(g(n)).$$

- Theorem. $\mathrm{DTIME}(f(n)) \subsetneq \mathrm{DTIME}(g(n))$

  Proof. We'll prove with $f(n) = n$ and $g(n) = n^2$.

  TM D :

  1. On input x, compute $|x|^2$.
  2. Simulate M_x on x for $|x|^2$ steps.
     a. If M_x stops and outputs b then output $1\text{-}b$.
     b. Otherwise, output 1.

Time Hierarchy Theorem

- Let $f(n)$ and $g(n)$ be time-constructible functions s.t.,

$$f(n) \,.\, \log f(n) = o(g(n)).$$

- Theorem. $\mathrm{DTIME}(f(n)) \subsetneq \mathrm{DTIME}(g(n))$

  Proof. We'll prove with $f(n) = n$ and $g(n) = n^2$.

  TM D :

  1. On input x, compute $|x|^2$.
  2. Simulate M_x on x for $|x|^2$ steps.
     a. If M_x stops and outputs b then output $1\text{-}b$.
     b. Otherwise, output 1.

D outputs the **opposite** of what M_x outputs.

Time Hierarchy Theorem

- Let $f(n)$ and $g(n)$ be time-constructible functions s.t.,

$$f(n) \,.\, \log f(n) = o(g(n)).$$

- Theorem. $\mathrm{DTIME}(f(n)) \subsetneq \mathrm{DTIME}(g(n))$

  Proof. We'll prove with $f(n) = n$ and $g(n) = n^2$.

  D runs in $O(n^2)$ time as n^2 is <u>time-constructible</u>.

Time Hierarchy Theorem

- Let $f(n)$ and $g(n)$ be time-constructible functions s.t.,

  $f(n) \,.\, \log f(n) = o(g(n))$.

- Theorem. $\mathrm{DTIME}(f(n)) \subsetneq \mathrm{DTIME}(g(n))$

  Proof. We'll prove with $f(n) = n$ and $g(n) = n^2$.

  Claim. There's no TM M with running time $O(n)$ that decides L (the language accepted by D).

Time Hierarchy Theorem

- Let $f(n)$ and $g(n)$ be time-constructible functions s.t.,

  $$f(n) \,.\, \log f(n) = o(g(n)).$$

- Theorem. $\mathrm{DTIME}(f(n)) \subsetneq \mathrm{DTIME}(g(n))$

  Proof. We'll prove with $f(n) = n$ and $g(n) = n^2$.

  - For contradiction, suppose M decides L and runs for at most $c.n$ steps on inputs of length n. (i.e., $M(x) = D(x)$ for all x)

Time Hierarchy Theorem

- Let $f(n)$ and $g(n)$ be time-constructible functions s.t.,

$$f(n) \, . \log f(n) = o(g(n)).$$

- Theorem. $\mathrm{DTIME}(f(n)) \subsetneq \mathrm{DTIME}(g(n))$

  Proof. We'll prove with $f(n) = n$ and $g(n) = n^2$.

  - For contradiction, suppose M decides L and runs for at most $c.n$ steps on inputs of length n. (i.e., $M(x) = D(x)$ for all x)

c is a constant

Time Hierarchy Theorem

- Let $f(n)$ and $g(n)$ be time-constructible functions s.t.,

$$f(n) \,.\, \log f(n) = o(g(n)).$$

- Theorem. $\mathrm{DTIME}(f(n)) \subsetneq \mathrm{DTIME}(g(n))$

  Proof. We'll prove with $f(n) = n$ and $g(n) = n^2$.

  - For contradiction, suppose M decides L and runs for at most $c.n$ steps on inputs of length n. (i.e., $M(x) = D(x)$ for all x)
  - Think of a <u>sufficiently large</u> x such that $M = M_x$.

Time Hierarchy Theorem

- Let $f(n)$ and $g(n)$ be time-constructible functions s.t.,

  $$f(n) \,.\, \log f(n) = o(g(n)).$$

- Theorem. $\mathrm{DTIME}(f(n)) \subsetneq \mathrm{DTIME}(g(n))$

  Proof. We'll prove with $f(n) = n$ and $g(n) = n^2$.

  - For contradiction, suppose M decides L and runs for at most $c.n$ steps on inputs of length n. (i.e., $M(x) = D(x)$ for all x)
  - Think of a sufficiently large x such that $M = M_x$.
  - Suppose $M(x) = M_x(x) = b$.

Time Hierarchy Theorem

- Let $f(n)$ and $g(n)$ be time-constructible functions s.t.,

$$f(n) \,.\, \log f(n) = o(g(n)).$$

- Theorem. $\text{DTIME}(f(n)) \subsetneq \text{DTIME}(g(n))$

  Proof. We'll prove with $f(n) = n$ and $g(n) = n^2$.

  - For contradiction, suppose M decides L and runs for at most $c.n$ steps on inputs of length n. (i.e., $M(x) = D(x)$ for all x)
  - Think of a <u>sufficiently large</u> x such that $M = M_x$.
  - Suppose $M(x) = M_x(x) = b$.
  - D on input x, simulates M_x on x for $|x|^2$ steps.

Time Hierarchy Theorem

- Let $f(n)$ and $g(n)$ be time-constructible functions s.t.,

$$f(n) \,.\, \log f(n) = o(g(n)).$$

- Theorem. $\mathrm{DTIME}(f(n)) \subsetneq \mathrm{DTIME}(g(n))$

  Proof. We'll prove with $f(n) = n$ and $g(n) = n^2$.

  - For contradiction, suppose M decides L and runs for at most $c.n$ steps on inputs of length n. (i.e., $M(x) = D(x)$ for all x)
  - Think of a sufficiently large x such that $M = M_x$.
  - Suppose $M(x) = M_x(x) = b$.
  - D on input x, simulates M_x on x for $|x|^2$ steps. Since M_x stops within $c.|x|$ steps, D's simulation also stops within $c'.c.\,|x|.\log|x|$ steps.

c' is a constant

Time Hierarchy Theorem

- Let $f(n)$ and $g(n)$ be time-constructible functions s.t.,

$$f(n) \,.\, \log f(n) = o(g(n)).$$

- Theorem. $DTIME(f(n)) \subsetneq DTIME(g(n))$

  Proof. We'll prove with $f(n) = n$ and $g(n) = n^2$.

  - For contradiction, suppose M decides L and runs for at most $c.n$ steps on inputs of length n. (i.e., $M(x) = D(x)$ for all x)
  - Think of a <u>sufficiently large</u> x such that $M = M_x$.
  - Suppose $M(x) = M_x(x) = b$.
  - D on input x, simulates M_x on x for $|x|^2$ steps. Since M_x stops within $c.|x|$ steps, D's simulation also stops within $c'.c.\,|x|.\log |x|$ steps. (as $c'.c.\,|x|.\log |x| < |x|^2$ for <u>sufficiently large</u> x)

Time Hierarchy Theorem

- Let $f(n)$ and $g(n)$ be time-constructible functions s.t.,

$$f(n) \,.\, \log f(n) = o(g(n)).$$

- Theorem. $\mathrm{DTIME}(f(n)) \subsetneq \mathrm{DTIME}(g(n))$

  Proof. We'll prove with $f(n) = n$ and $g(n) = n^2$.

  - For contradiction, suppose M decides L and runs for at most $c.n$ steps on inputs of length n. (i.e., $M(x) = D(x)$ for all x)
  - Think of a <u>sufficiently large</u> x such that $M = M_x$.
  - Suppose $M(x) = M_x(x) = b$.
  - D on input x, simulates M_x on x for $|x|^2$ steps. Since M_x stops within $c.|x|$ steps, D's simulation also stops within $c'.c.\,|x|.\log |x|$ steps. And D outputs the **opposite** of what M_x outputs!

Time Hierarchy Theorem

- Let $f(n)$ and $g(n)$ be time-constructible functions s.t.,

$$f(n)\,.\log f(n) = o(g(n)).$$

- Theorem. $\mathrm{DTIME}(f(n)) \subsetneq \mathrm{DTIME}(g(n))$

  Proof. We'll prove with $f(n) = n$ and $g(n) = n^2$.

  - For contradiction, suppose M decides L and runs for at most $c.n$ steps on inputs of length n. (i.e., $M(x) = D(x)$ for all x)
  - Think of a <u>sufficiently large</u> x such that $M = M_x$.
  - Suppose $M(x) = M_x(x) = b$.
  - Hence, $D(x) = 1\text{-}b$.

Time Hierarchy Theorem

- Let $f(n)$ and $g(n)$ be time-constructible functions s.t.,

$$f(n) \,.\, \log f(n) = o(g(n)).$$

- Theorem. $DTIME(f(n)) \subsetneq DTIME(g(n))$

  Proof. We'll prove with $f(n) = n$ and $g(n) = n^2$.

  - For contradiction, suppose M decides L and runs for at most $c.n$ steps on inputs of length n. $\boxed{\text{(i.e., } M(x) = D(x) \text{ for all } x\text{)}}$
  - Think of a <u>sufficiently large</u> x such that $M = M_x$.
  - Suppose $M(x) = M_x(x) = b$.
  - Hence, $D(x) = 1\text{-}b$.

Contradiction! M does not decide L.

Time Hierarchy Theorem

- Let $f(n)$ and $g(n)$ be time-constructible functions s.t.,

  $$f(n) \,.\, \log f(n) = o(g(n)).$$

- Theorem. $\mathrm{DTIME}(f(n)) \subsetneq \mathrm{DTIME}(g(n))$

- Theorem. $\mathrm{P} \subsetneq \mathrm{EXP}$

  Proof. Similar (homework)

Time Hierarchy Theorem

- Is there a natural problem that takes close to n^2 time?

Time Hierarchy Theorem

- Is there a natural problem that takes close to n^2 time?
- 3SUM: Given a list of n numbers, check if there exists 3 numbers in the list that sum to zero.

Time Hierarchy Theorem

- Is there a natural problem that takes close to n^2 time?

- 3SUM: Given a list of n numbers, check if there exists 3 numbers in the list that sum to zero.
- Conjecture. ***No*** algorithm solves 3SUM in $O(n^{2-\varepsilon})$ time for some constant $\varepsilon > 0$.

Time Hierarchy Theorem

- Is there a natural problem that takes close to n^2 time?

- 3SUM: Given a list of n numbers, check if there exists 3 numbers in the list that sum to zero.
- Conjecture. ***No*** algorithm solves 3SUM in $O(n^{2-\varepsilon})$ time for some constant $\varepsilon > 0$.

- However, there's a $\sim O(n^2 / (\log n)^2)$ time algorithm for 3SUM. ("$\sim$" suppressing a poly(log log n) factor.)

Time Hierarchy Theorem

- Is there a natural problem that takes close to n^2 time?

- 3SUM: Given a list of n numbers, check if there exists 3 numbers in the list that sum to zero.
- Conjecture. ***No*** algorithm solves 3SUM in $O(n^{2-\varepsilon})$ time for some constant $\varepsilon > 0$.
- kSUM: Given a list of n numbers, check if there exists k numbers in the list that sum to zero.

Time Hierarchy Theorem

- Is there a natural problem that takes close to n^2 time?

- 3SUM: Given a list of n numbers, check if there exists 3 numbers in the list that sum to zero.
- Conjecture. ***No*** algorithm solves 3SUM in $O(n^{2-\varepsilon})$ time for some constant $\varepsilon > 0$.
- kSUM: Given a list of n numbers, check if there exists k numbers in the list that sum to zero.
- Theorem *(Patrascu & Williams 2010)*. ETH implies kSUM requires $n^{\Omega(k)}$ time.