Lecture 29

Uniform Circuits, TMs with Advice, Karp-Lipton Theorem

Uniformly Generated Circuits

Uniformly Generated Circuits

Definition: A circuit family $\{C_n\}$ is **P-uniform**

Uniformly Generated Circuits

Definition: A circuit family $\{C_n\}$ is **P-uniform** if there is a polynomial-time TM that on input 1^n

Uniformly Generated Circuits

Definition: A circuit family $\{C_n\}$ is **P-uniform** if there is a polynomial-time TM that on input 1^n outputs the description of the circuit C_n.

Uniformly Generated Circuits

Definition: A circuit family $\{C_n\}$ is **P-uniform** if there is a polynomial-time TM that on input 1^n outputs the description of the circuit C_n.

Theorem: A language L is computable by a **P-uniform** circuit family iff $L \in$ **P**.

Uniformly Generated Circuits

Definition: A circuit family $\{C_n\}$ is **P-uniform** if there is a polynomial-time TM that on input 1^n outputs the description of the circuit C_n.

Theorem: A language L is computable by a **P-uniform** circuit family iff $L \in$ **P**.

Proof:

Uniformly Generated Circuits

Definition: A circuit family $\{C_n\}$ is **P-uniform** if there is a polynomial-time TM that on input 1^n outputs the description of the circuit C_n.

Theorem: A language L is computable by a **P-uniform** circuit family iff $L \in$ **P**.

Proof: ($\implies$) Let L be a language computable by a **P-uniform** circuit family.

Uniformly Generated Circuits

Definition: A circuit family $\{C_n\}$ is **P-uniform** if there is a polynomial-time TM that on input 1^n outputs the description of the circuit C_n.

Theorem: A language L is computable by a **P-uniform** circuit family iff $L \in$ **P**.

Proof: ($\Longrightarrow$) Let L be a language computable by a **P-uniform** circuit family.

Polytime TM M that decides L on input x:

Uniformly Generated Circuits

Definition: A circuit family $\{C_n\}$ is **P-uniform** if there is a polynomial-time TM that on input 1^n outputs the description of the circuit C_n.

Theorem: A language L is computable by a **P-uniform** circuit family iff $L \in$ **P**.

Proof: ($\Longrightarrow$) Let L be a language computable by a **P-uniform** circuit family.

Polytime TM M that decides L on input x: Generates $C_{|x|}$ and outputs $C_{|x|}(x)$.

Uniformly Generated Circuits

Definition: A circuit family $\{C_n\}$ is **P-uniform** if there is a polynomial-time TM that on input 1^n outputs the description of the circuit C_n.

Theorem: A language L is computable by a **P-uniform** circuit family iff $L \in$ **P**.

Proof: ($\implies$) Let L be a language computable by a **P-uniform** circuit family.

Polytime TM M that decides L on input x: Generates $C_{|x|}$ and outputs $C_{|x|}(x)$.

($\impliedby$)

Uniformly Generated Circuits

Definition: A circuit family $\{C_n\}$ is **P-uniform** if there is a polynomial-time TM that on input 1^n outputs the description of the circuit C_n.

Theorem: A language L is computable by a **P-uniform** circuit family iff $L \in$ **P**.

Proof: ($\Longrightarrow$) Let L be a language computable by a **P-uniform** circuit family.

Polytime TM M that decides L on input x: Generates $C_{|x|}$ and outputs $C_{|x|}(x)$.

($\Longleftarrow$) **Idea:** Circuit construction in proof of **P** $\subseteq$ **P/poly** is doable in polynomial time.

Uniformly Generated Circuits

Definition: A circuit family $\{C_n\}$ is **P-uniform** if there is a polynomial-time TM that on input 1^n outputs the description of the circuit C_n.

Theorem: A language L is computable by a **P-uniform** circuit family iff $L \in$ **P**.

Proof: ($\Longrightarrow$) Let L be a language computable by a **P-uniform** circuit family.

Polytime TM M that decides L on input x: Generates $C_{|x|}$ and outputs $C_{|x|}(x)$.

($\Longleftarrow$) **Idea:** Circuit construction in proof of **P** $\subseteq$ **P/poly** is doable in polynomial time. ∎

Uniformly Generated Circuits

Uniformly Generated Circuits

Definition: A circuit family $\{C_n\}$ is **logspace-uniform** if there is an implicitly logspace computable

Uniformly Generated Circuits

Definition: A circuit family $\{C_n\}$ is **logspace-uniform** if there is an implicitly logspace computable function f that maps 1^n to the description of the circuit C_n.

Uniformly Generated Circuits

Definition: A circuit family $\{C_n\}$ is **logspace-uniform** if there is an implicitly logspace computable function f that maps 1^n to the description of the circuit C_n.

Theorem: A language L is computable by a **logspace-uniform** circuit family iff $L \in$ **P**.

Uniformly Generated Circuits

Definition: A circuit family $\{C_n\}$ is **logspace-uniform** if there is an implicitly logspace computable function f that maps 1^n to the description of the circuit C_n.

Theorem: A language L is computable by a **logspace-uniform** circuit family iff $L \in$ **P**.

Proof: ($\Longrightarrow$)

Uniformly Generated Circuits

Definition: A circuit family $\{C_n\}$ is **logspace-uniform** if there is an implicitly logspace computable function f that maps 1^n to the description of the circuit C_n.

Theorem: A language L is computable by a **logspace-uniform** circuit family iff $L \in$ **P**.

Proof: ($\Longrightarrow$) Similar to the proof of the previous theorem.

Uniformly Generated Circuits

Definition: A circuit family $\{C_n\}$ is **logspace-uniform** if there is an implicitly logspace computable function f that maps 1^n to the description of the circuit C_n.

Theorem: A language L is computable by a **logspace-uniform** circuit family iff $L \in$ **P**.

Proof: ($\Longrightarrow$) Similar to the proof of the previous theorem.

($\Longleftarrow$)

Uniformly Generated Circuits

Definition: A circuit family $\{C_n\}$ is **logspace-uniform** if there is an implicitly logspace computable function f that maps 1^n to the description of the circuit C_n.

Theorem: A language L is computable by a **logspace-uniform** circuit family iff $L \in$ **P**.

Proof: ($\Longrightarrow$) Similar to the proof of the previous theorem.

($\Longleftarrow$) We use the fact that circuit construction in **P** $\subseteq$ **P/poly** is logspace computable.

Uniformly Generated Circuits

Definition: A circuit family $\{C_n\}$ is **logspace-uniform** if there is an implicitly logspace computable function f that maps 1^n to the description of the circuit C_n.

Theorem: A language L is computable by a **logspace-uniform** circuit family iff $L \in \mathsf{P}$.

Proof: ($\Longrightarrow$) Similar to the proof of the previous theorem.

($\Longleftarrow$) We use the fact that circuit construction in $\mathsf{P} \subseteq \mathsf{P}_{/\mathsf{poly}}$ is logspace computable. ■

TMs with Advice

TMs with Advice

Idea: An advice α_n for a TM on all inputs of length n.

TMs with Advice

Idea: An advice α_n for a TM on all inputs of length n.

Definition: Let $T, A : \mathbb{N} \to \mathbb{N}$ be functions.

TMs with Advice

Idea: An advice α_n for a TM on all inputs of length n.

Definition: Let $T, A : \mathbb{N} \to \mathbb{N}$ be functions. A language L is in $\mathsf{DTIME}(T(n))/A(n)$,

TMs with Advice

Idea: An advice α_n for a TM on all inputs of length n.

Definition: Let $T, A : \mathbb{N} \to \mathbb{N}$ be functions. A language L is in DTIME$(T(n))/A(n)$, if $\exists$ a $T(n)$-time

TMs with Advice

Idea: An advice α_n for a TM on all inputs of length n.

Definition: Let $T, A : \mathbb{N} \to \mathbb{N}$ be functions. A language L is in $\mathsf{DTIME}(T(n))/A(n)$, if $\exists$ a $T(n)$-time TM M

TMs with Advice

Idea: An advice α_n for a TM on all inputs of length n.

Definition: Let $T, A : \mathbb{N} \to \mathbb{N}$ be functions. A language L is in $\mathsf{DTIME}(T(n))/A(n)$, if $\exists$ a $T(n)$-time TM M and sequence of strings $\{\alpha_n\}_{n \in \mathbb{N}}$

TMs with Advice

Idea: An advice α_n for a TM on all inputs of length n.

Definition: Let $T, A : \mathbb{N} \to \mathbb{N}$ be functions. A language L is in $\mathsf{DTIME}(T(n))/A(n)$, if $\exists$ a $T(n)$-time TM M and sequence of strings $\{\alpha_n\}_{n\in\mathbb{N}}$ with $\alpha_n \in \{0,1\}^{A(n)}$

TMs with Advice

Idea: An advice α_n for a TM on all inputs of length n.

Definition: Let $T, A : \mathbb{N} \to \mathbb{N}$ be functions. A language L is in $\mathsf{DTIME}(T(n))/A(n)$, if $\exists$ a $T(n)$-time TM M and sequence of strings $\{\alpha_n\}_{n\in\mathbb{N}}$ with $\alpha_n \in \{0,1\}^{A(n)}$ such that $\forall x \in \{0,1\}^n$,

TMs with Advice

Idea: An advice α_n for a TM on all inputs of length n.

Definition: Let $T, A : \mathbb{N} \to \mathbb{N}$ be functions. A language L is in $\mathsf{DTIME}(T(n))/A(n)$, if $\exists$ a $T(n)$-time TM M and sequence of strings $\{\alpha_n\}_{n \in \mathbb{N}}$ with $\alpha_n \in \{0,1\}^{A(n)}$ such that $\forall x \in \{0,1\}^n$,

$$x \in L \iff M(x, \alpha_n) = 1$$

TMs with Advice

Idea: An advice α_n for a TM on all inputs of length n.

Definition: Let $T, A : \mathbb{N} \to \mathbb{N}$ be functions. A language L is in DTIME$(T(n))/A(n)$, if $\exists$ a $T(n)$-time TM M and sequence of strings $\{\alpha_n\}_{n\in\mathbb{N}}$ with $\alpha_n \in \{0,1\}^{A(n)}$ such that $\forall x \in \{0,1\}^n$,

$$x \in L \iff M(x, \alpha_n) = 1$$

Example: *UHALT* is has a _____ time TM with advice strings of length _.

TMs with Advice

Idea: An advice α_n for a TM on all inputs of length n.

Definition: Let $T, A : \mathbb{N} \to \mathbb{N}$ be functions. A language L is in **DTIME**$(T(n))/A(n)$, if $\exists$ a $T(n)$-time TM M and sequence of strings $\{\alpha_n\}_{n\in\mathbb{N}}$ with $\alpha_n \in \{0,1\}^{A(n)}$ such that $\forall x \in \{0,1\}^n$,

$$x \in L \iff M(x, \alpha_n) = 1$$

Example: *UHALT* is has a linear time TM with advice strings of length _.

TMs with Advice

Idea: An advice α_n for a TM on all inputs of length n.

Definition: Let $T, A : \mathbb{N} \to \mathbb{N}$ be functions. A language L is in **DTIME**$(T(n))/A(n)$, if $\exists$ a $T(n)$-time TM M and sequence of strings $\{\alpha_n\}_{n\in\mathbb{N}}$ with $\alpha_n \in \{0,1\}^{A(n)}$ such that $\forall x \in \{0,1\}^n$,

$$x \in L \iff M(x, \alpha_n) = 1$$

Example: *UHALT* is has a linear time TM with advice strings of length 1.

TMs with Advice

Idea: An advice α_n for a TM on all inputs of length n.

Definition: Let $T, A : \mathbb{N} \to \mathbb{N}$ be functions. A language L is in **DTIME**$(T(n))/A(n)$, if $\exists$ a $T(n)$-time TM M and sequence of strings $\{\alpha_n\}_{n\in\mathbb{N}}$ with $\alpha_n \in \{0,1\}^{A(n)}$ such that $\forall x \in \{0,1\}^n$,

$$x \in L \iff M(x, \alpha_n) = 1$$

Example: *UHALT* is has a linear time TM with advice strings of length 1.

TM M that decides *UHALT* on input x:

TMs with Advice

Idea: An advice α_n for a TM on all inputs of length n.

Definition: Let $T, A : \mathbb{N} \to \mathbb{N}$ be functions. A language L is in **DTIME**$(T(n))/A(n)$, if $\exists$ a $T(n)$-time TM M and sequence of strings $\{\alpha_n\}_{n\in\mathbb{N}}$ with $\alpha_n \in \{0,1\}^{A(n)}$ such that $\forall x \in \{0,1\}^n$,

$$x \in L \iff M(x, \alpha_n) = 1$$

Example: *UHALT* is has a linear time TM with advice strings of length 1.

TM M that decides *UHALT* on input x:

1) Rejects if x is not all 1s.

TMs with Advice

Idea: An advice α_n for a TM on all inputs of length n.

Definition: Let $T, A : \mathbb{N} \to \mathbb{N}$ be functions. A language L is in DTIME$(T(n))/A(n)$, if $\exists$ a $T(n)$-time TM M and sequence of strings $\{\alpha_n\}_{n\in\mathbb{N}}$ with $\alpha_n \in \{0,1\}^{A(n)}$ such that $\forall x \in \{0,1\}^n$,

$$x \in L \iff M(x, \alpha_n) = 1$$

Example: *UHALT* is has a linear time TM with advice strings of length 1.

TM M that decides *UHALT* on input x:

1) Rejects if x is not all 1s.

2) Accepts when x is all 1s if and only if advice is 1.

TMs with Advice

TMs with Advice

Theorem: $\mathsf{P}_{/\mathsf{poly}} = \cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d$.

TMs with Advice

Theorem: $\mathsf{P}_{/\mathsf{poly}} = \cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d$.

Proof:

TMs with Advice

Theorem: $\mathsf{P}_{/\mathsf{poly}} = \cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d$.

Proof: $\mathsf{P}_{/\mathsf{poly}} \subseteq \cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d$:

TMs with Advice

Theorem: $\mathsf{P}_{/\mathsf{poly}} = \cup_{c,d}\,\mathsf{DTIME}(n^c)/n^d$.

Proof: $\mathsf{P}_{/\mathsf{poly}} \subseteq \cup_{c,d}\,\mathsf{DTIME}(n^c)/n^d$:

Let $L \in \mathsf{P}_{/\mathsf{poly}}$

TMs with Advice

Theorem: $\mathsf{P}_{/\mathsf{poly}} = \cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d$.

Proof: $\mathsf{P}_{/\mathsf{poly}} \subseteq \cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d$:

Let $L \in \mathsf{P}_{/\mathsf{poly}}$ and $\{C_n\}$ be its polysize circuit family.

TMs with Advice

Theorem: $\mathsf{P}_{/\mathsf{poly}} = \cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d$.

Proof: $\mathsf{P}_{/\mathsf{poly}} \subseteq \cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d$:

Let $L \in \mathsf{P}_{/\mathsf{poly}}$ and $\{C_n\}$ be its polysize circuit family.

Polynomial-time TM M that decides L on input x and advice

TMs with Advice

Theorem: $\mathsf{P}_{/\mathsf{poly}} = \cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d$.

Proof: $\mathsf{P}_{/\mathsf{poly}} \subseteq \cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d$:

Let $L \in \mathsf{P}_{/\mathsf{poly}}$ and $\{C_n\}$ be its polysize circuit family.

Polynomial-time TM M that decides L on input x and advice $C_{|x|}$

TMs with Advice

Theorem: $\mathsf{P}_{/\mathsf{poly}} = \cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d$.

Proof: $\mathsf{P}_{/\mathsf{poly}} \subseteq \cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d$:

Let $L \in \mathsf{P}_{/\mathsf{poly}}$ and $\{C_n\}$ be its polysize circuit family.

Polynomial-time TM M that decides L on input x and advice $C_{|x|}$ outputs $C_{|x|}(x)$.

TMs with Advice

Theorem: $\mathsf{P}_{/\mathsf{poly}} = \cup_{c,d} \mathsf{DTIME}(n^c)/n^d$.

Proof: $\mathsf{P}_{/\mathsf{poly}} \subseteq \cup_{c,d} \mathsf{DTIME}(n^c)/n^d$:

Let $L \in \mathsf{P}_{/\mathsf{poly}}$ and $\{C_n\}$ be its polysize circuit family.

Polynomial-time TM M that decides L on input x and advice $C_{|x|}$ outputs $C_{|x|}(x)$.

$\cup_{c,d} \mathsf{DTIME}(n^c)/n^d \subseteq \mathsf{P}_{/\mathsf{poly}}$:

TMs with Advice

Theorem: $\mathsf{P}_{/\mathsf{poly}} = \cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d$.

Proof: $\mathsf{P}_{/\mathsf{poly}} \subseteq \cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d$:

Let $L \in \mathsf{P}_{/\mathsf{poly}}$ and $\{C_n\}$ be its polysize circuit family.

Polynomial-time TM M that decides L on input x and advice $C_{|x|}$ outputs $C_{|x|}(x)$.

$\cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d \subseteq \mathsf{P}_{/\mathsf{poly}}$:

Let $L \in \cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d$

TMs with Advice

Theorem: $\mathsf{P}_{/\mathsf{poly}} = \cup_{c,d}\,\mathsf{DTIME}(n^c)/n^d$.

Proof: $\mathsf{P}_{/\mathsf{poly}} \subseteq \cup_{c,d}\,\mathsf{DTIME}(n^c)/n^d$:

Let $L \in \mathsf{P}_{/\mathsf{poly}}$ and $\{C_n\}$ be its polysize circuit family.

Polynomial-time TM M that decides L on input x and advice $C_{|x|}$ outputs $C_{|x|}(x)$.

$\cup_{c,d}\,\mathsf{DTIME}(n^c)/n^d \subseteq \mathsf{P}_{/\mathsf{poly}}$:

Let $L \in \cup_{c,d}\,\mathsf{DTIME}(n^c)/n^d$ and M be its polytime TM with advice string sequence $\{\alpha_n\}$.

TMs with Advice

Theorem: $\mathsf{P}_{/\mathsf{poly}} = \cup_{c,d}\,\mathsf{DTIME}(n^c)/n^d$.

Proof: $\mathsf{P}_{/\mathsf{poly}} \subseteq \cup_{c,d}\,\mathsf{DTIME}(n^c)/n^d$:

Let $L \in \mathsf{P}_{/\mathsf{poly}}$ and $\{C_n\}$ be its polysize circuit family.

Polynomial-time TM M that decides L on input x and advice $C_{|x|}$ outputs $C_{|x|}(x)$.

$\cup_{c,d}\,\mathsf{DTIME}(n^c)/n^d \subseteq \mathsf{P}_{/\mathsf{poly}}$:

Let $L \in \cup_{c,d}\,\mathsf{DTIME}(n^c)/n^d$ and M be its polytime TM with advice string sequence $\{\alpha_n\}$.

There exists a polysize circuit D_n such that $\forall x \in \{0,1\}^n$ and $\forall \alpha \in \{0,1\}^{poly(n)}$

TMs with Advice

Theorem: $\mathsf{P}_{/\mathsf{poly}} = \cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d$.

Proof: $\mathsf{P}_{/\mathsf{poly}} \subseteq \cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d$:

Let $L \in \mathsf{P}_{/\mathsf{poly}}$ and $\{C_n\}$ be its polysize circuit family.

Polynomial-time TM M that decides L on input x and advice $C_{|x|}$ outputs $C_{|x|}(x)$.

$\cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d \subseteq \mathsf{P}_{/\mathsf{poly}}$:

Let $L \in \cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d$ and M be its polytime TM with advice string sequence $\{\alpha_n\}$.

There exists a polysize circuit D_n such that $\forall x \in \{0,1\}^n$ and $\forall \alpha \in \{0,1\}^{poly(n)}$

$$M(x, \alpha) = D_n(x, \alpha)$$

TMs with Advice

Theorem: $\mathsf{P}_{/\mathsf{poly}} = \cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d$.

Proof: $\mathsf{P}_{/\mathsf{poly}} \subseteq \cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d$:

Let $L \in \mathsf{P}_{/\mathsf{poly}}$ and $\{C_n\}$ be its polysize circuit family.

Polynomial-time TM M that decides L on input x and advice $C_{|x|}$ outputs $C_{|x|}(x)$.

$\cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d \subseteq \mathsf{P}_{/\mathsf{poly}}$:

Let $L \in \cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d$ and M be its polytime TM with advice string sequence $\{\alpha_n\}$.

There exists a polysize circuit D_n such that $\forall x \in \{0,1\}^n$ and $\forall \alpha \in \{0,1\}^{poly(n)}$

$$M(x, \alpha) = D_n(x, \alpha)$$

Then, polysize circuit C_n for L is D_n with α_n hard-wired as second input.

TMs with Advice

Theorem: $\mathsf{P}_{/\mathsf{poly}} = \cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d$.

Proof: $\mathsf{P}_{/\mathsf{poly}} \subseteq \cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d$:

Let $L \in \mathsf{P}_{/\mathsf{poly}}$ and $\{C_n\}$ be its polysize circuit family.

Polynomial-time TM M that decides L on input x and advice $C_{|x|}$ outputs $C_{|x|}(x)$.

$\cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d \subseteq \mathsf{P}_{/\mathsf{poly}}$:

Let $L \in \cup_{c,d}\, \mathsf{DTIME}(n^c)/n^d$ and M be its polytime TM with advice string sequence $\{\alpha_n\}$.

There exists a polysize circuit D_n such that $\forall x \in \{0,1\}^n$ and $\forall \alpha \in \{0,1\}^{poly(n)}$

$$M(x, \alpha) = D_n(x, \alpha)$$

Then, polysize circuit C_n for L is D_n with α_n hard-wired as second input. ■

Karp-Lipton Theorem

Karp-Lipton Theorem

Theorem: If $\mathsf{NP} \subseteq \mathsf{P}_{/\mathsf{poly}}$, then $\mathsf{PH} = \Sigma_2^p$.

Karp-Lipton Theorem

Theorem: If $\mathsf{NP} \subseteq \mathsf{P}_{/\mathsf{poly}}$, then $\mathsf{PH} = \Sigma_2^p$.

Proof:

Karp-Lipton Theorem

Theorem: If $\mathsf{NP} \subseteq \mathsf{P}_{/\mathsf{poly}}$, then $\mathsf{PH} = \Sigma_2^p$.

Proof: We will prove that if $SAT \in \mathsf{P}_{/\mathsf{poly}}$, then $\Pi_2^p \subseteq \Sigma_2^p$.

Karp-Lipton Theorem

Theorem: If $\mathsf{NP} \subseteq \mathsf{P}_{/\mathsf{poly}}$, then $\mathsf{PH} = \Sigma_2^p$.

Proof: We will prove that if $SAT \in \mathsf{P}_{/\mathsf{poly}}$, then $\Pi_2^p \subseteq \Sigma_2^p$. ($\mathsf{coC} \subseteq \mathsf{C} \implies \mathsf{C} = \mathsf{coC}$.)

Karp-Lipton Theorem

Theorem: If $\mathsf{NP} \subseteq \mathsf{P}_{/\mathsf{poly}}$, then $\mathsf{PH} = \Sigma_2^p$.

Proof: We will prove that if $SAT \in \mathsf{P}_{/\mathsf{poly}}$, then $\Pi_2^p \subseteq \Sigma_2^p$. ($\mathsf{coC} \subseteq \mathsf{C} \Longrightarrow \mathsf{C} = \mathsf{coC}$.)

Let $L \in \Pi_2^p$.

Karp-Lipton Theorem

Theorem: If $\mathsf{NP} \subseteq \mathsf{P}_{/\mathsf{poly}}$, then $\mathsf{PH} = \Sigma_2^p$.

Proof: We will prove that if $SAT \in \mathsf{P}_{/\mathsf{poly}}$, then $\Pi_2^p \subseteq \Sigma_2^p$. ($\mathsf{coC} \subseteq \mathsf{C} \Longrightarrow \mathsf{C} = \mathsf{coC}$.)

Let $L \in \Pi_2^p$. Then, $\exists$ a polytime TM M such that

Karp-Lipton Theorem

Theorem: If NP $\subseteq$ P$_{/\text{poly}}$, then PH $= \Sigma_2^p$.

Proof: We will prove that if *SAT* $\in$ P$_{/\text{poly}}$, then $\Pi_2^p \subseteq \Sigma_2^p$. (coC $\subseteq$ C $\implies$ C $=$ coC.)

Let $L \in \Pi_2^p$. Then, $\exists$ a polytime TM M such that

$$x \in L \iff \forall u_1 \exists u_2 \text{ such that } M(x, u_1, u_2) = 1$$

Karp-Lipton Theorem

Theorem: If NP $\subseteq$ P$_{/\text{poly}}$, then PH $= \Sigma_2^p$.

Proof: We will prove that if $SAT \in$ P$_{/\text{poly}}$, then $\Pi_2^p \subseteq \Sigma_2^p$. (coC $\subseteq$ C $\implies$ C $=$ coC.)

Let $L \in \Pi_2^p$. Then, $\exists$ a polytime TM M such that

$$x \in L \iff \forall u_1 \exists u_2 \text{ such that } M(x, u_1, u_2) = 1$$

Define a related language L'

Karp-Lipton Theorem

Theorem: If $\mathsf{NP} \subseteq \mathsf{P}_{/\mathsf{poly}}$, then $\mathsf{PH} = \Sigma_2^p$.

Proof: We will prove that if $SAT \in \mathsf{P}_{/\mathsf{poly}}$, then $\Pi_2^p \subseteq \Sigma_2^p$. ($\mathsf{coC} \subseteq \mathsf{C} \implies \mathsf{C} = \mathsf{coC}$.)

Let $L \in \Pi_2^p$. Then, $\exists$ a polytime TM M such that

$$x \in L \iff \forall u_1 \exists u_2 \text{ such that } M(x, u_1, u_2) = 1$$

Define a related language L'

$$(x, u_1) \in L' \iff \exists u_2 \text{ s.t. } M(x, u_1, u_2) = 1$$

Karp-Lipton Theorem

Theorem: If NP $\subseteq$ P$_{/\text{poly}}$, then PH $= \Sigma_2^p$.

Proof: We will prove that if *SAT* $\in$ P$_{/\text{poly}}$, then $\Pi_2^p \subseteq \Sigma_2^p$. (coC $\subseteq$ C $\Longrightarrow$ C $=$ coC.)

Let $L \in \Pi_2^p$. Then, $\exists$ a polytime TM M such that

$$x \in L \iff \forall u_1 \exists u_2 \text{ such that } M(x, u_1, u_2) = 1$$

Define a related language L'

$$(x, u_1) \in L' \iff \exists u_2 \text{ s.t. } M(x, u_1, u_2) = 1$$

$L' \in$ NP.

Karp-Lipton Theorem

Theorem: If NP $\subseteq$ P$_{/\text{poly}}$, then PH $= \Sigma_2^p$.

Proof: We will prove that if *SAT* $\in$ P$_{/\text{poly}}$, then $\Pi_2^p \subseteq \Sigma_2^p$. (coC $\subseteq$ C $\implies$ C $=$ coC.)

Let $L \in \Pi_2^p$. Then, $\exists$ a polytime TM M such that

$$x \in L \iff \forall u_1 \exists u_2 \text{ such that } M(x, u_1, u_2) = 1$$

Define a related language L'

$$(x, u_1) \in L' \iff \exists u_2 \text{ s.t. } M(x, u_1, u_2) = 1$$

$L' \in$ NP. Let f be the function reducing L' to *SAT*.

Karp-Lipton Theorem

Theorem: If $\mathsf{NP} \subseteq \mathsf{P}_{/\mathsf{poly}}$, then $\mathsf{PH} = \Sigma_2^p$.

Proof: We will prove that if *SAT* $\in \mathsf{P}_{/\mathsf{poly}}$, then $\Pi_2^p \subseteq \Sigma_2^p$. ($\mathsf{coC} \subseteq \mathsf{C} \implies \mathsf{C} = \mathsf{coC}$.)

Let $L \in \Pi_2^p$. Then, $\exists$ a polytime TM M such that

$$x \in L \iff \forall u_1 \exists u_2 \text{ such that } M(x, u_1, u_2) = 1$$

Define a related language L'

$$(x, u_1) \in L' \iff \exists u_2 \text{ s.t. } M(x, u_1, u_2) = 1$$

$L' \in \mathsf{NP}$. Let f be the function reducing L' to *SAT*.

Going back to L:

Karp-Lipton Theorem

Theorem: If NP $\subseteq$ P$_{/\text{poly}}$, then PH $= \Sigma_2^p$.

Proof: We will prove that if *SAT* $\in$ P$_{/\text{poly}}$, then $\Pi_2^p \subseteq \Sigma_2^p$. (coC $\subseteq$ C $\Longrightarrow$ C $=$ coC.)

Let $L \in \Pi_2^p$. Then, $\exists$ a polytime TM M such that

$$x \in L \iff \forall u_1 \exists u_2 \text{ such that } M(x, u_1, u_2) = 1$$

Define a related language L'

$$(x, u_1) \in L' \iff \exists u_2 \text{ s.t. } M(x, u_1, u_2) = 1$$

$L' \in$ NP. Let f be the function reducing L' to *SAT*.

Going back to L:

$$x \in L \iff \forall u_1\ (x, u_1) \in L'$$

Karp-Lipton Theorem

Theorem: If NP $\subseteq$ P$_{/\text{poly}}$, then PH $= \Sigma_2^p$.

Proof: We will prove that if *SAT* $\in$ P$_{/\text{poly}}$, then $\Pi_2^p \subseteq \Sigma_2^p$. (coC $\subseteq$ C $\Longrightarrow$ C $=$ coC.)

Let $L \in \Pi_2^p$. Then, $\exists$ a polytime TM M such that

$$x \in L \iff \forall u_1 \exists u_2 \text{ such that } M(x, u_1, u_2) = 1$$

Define a related language L'

$$(x, u_1) \in L' \iff \exists u_2 \text{ s.t. } M(x, u_1, u_2) = 1$$

$L' \in$ NP. Let f be the function reducing L' to *SAT*.

Going back to L:

$$x \in L \iff \forall u_1\ (x, u_1) \in L' \iff \forall u_1\ f(x, u_1) \in \mathit{SAT}$$

Karp-Lipton Theorem

Theorem: If NP $\subseteq$ P$_{/\text{poly}}$, then PH $= \Sigma_2^p$.

Proof: We will prove that if *SAT* $\in$ P$_{/\text{poly}}$, then $\Pi_2^p \subseteq \Sigma_2^p$. (coC $\subseteq$ C $\Longrightarrow$ C = coC.)

Let $L \in \Pi_2^p$. Then, $\exists$ a polytime TM M such that

$$x \in L \iff \forall u_1 \exists u_2 \text{ such that } M(x, u_1, u_2) = 1$$

Define a related language L'

$$(x, u_1) \in L' \iff \exists u_2 \text{ s.t. } M(x, u_1, u_2) = 1$$

$L' \in$ NP. Let f be the function reducing L' to *SAT*.

Going back to L:

$$x \in L \iff \forall u_1\ (x, u_1) \in L' \iff \forall u_1\ f(x, u_1) \in \mathit{SAT} \iff \exists C\, \forall u_1\ C(f(x, u_1)) = 1$$

Karp-Lipton Theorem

Theorem: If NP $\subseteq$ P$_{/\text{poly}}$, then PH $= \Sigma_2^p$.

Proof: We will prove that if *SAT* $\in$ P$_{/\text{poly}}$, then $\Pi_2^p \subseteq \Sigma_2^p$. (coC $\subseteq$ C $\Longrightarrow$ C $=$ coC.)

Let $L \in \Pi_2^p$. Then, $\exists$ a polytime TM M such that

$$x \in L \iff \forall u_1 \exists u_2 \text{ such that } M(x, u_1, u_2) = 1$$

Define a related language L'

$$(x, u_1) \in L' \iff \exists u_2 \text{ s.t. } M(x, u_1, u_2) = 1$$

$L' \in$ NP. Let f be the function reducing L' to *SAT*.

Going back to L:

$$x \in L \iff \forall u_1\ (x, u_1) \in L' \iff \forall u_1\ f(x, u_1) \in \mathit{SAT} \iff \exists C \forall u_1\ C(f(x, u_1)) = 1$$

($\because$ *SAT* $\in$ P$_{/\text{poly}}$)

Karp-Lipton Theorem

Theorem: If NP $\subseteq$ P$_{/\text{poly}}$, then PH $= \Sigma_2^p$.

Proof: We will prove that if *SAT* $\in$ P$_{/\text{poly}}$, then $\Pi_2^p \subseteq \Sigma_2^p$. (coC $\subseteq$ C $\implies$ C $=$ coC.)

Let $L \in \Pi_2^p$. Then, $\exists$ a polytime TM M such that

$$x \in L \iff \forall u_1 \exists u_2 \text{ such that } M(x, u_1, u_2) = 1$$

Define a related language L'

$$(x, u_1) \in L' \iff \exists u_2 \text{ s.t. } M(x, u_1, u_2) = 1$$

$L' \in$ NP. Let f be the function reducing L' to *SAT*.

Going back to L:

$$x \in L \iff \forall u_1\ (x, u_1) \in L' \iff \forall u_1\ f(x, u_1) \in \mathit{SAT} \iff \exists C \forall u_1\ C(f(x, u_1)) = 1$$

($\because$ *SAT* $\in$ P$_{/\text{poly}}$)

…

Karp-Lipton Theorem

Theorem: If NP $\subseteq$ P$_{/\text{poly}}$, then PH $= \Sigma_2^p$.

Proof: We will prove that if *SAT* $\in$ P$_{/\text{poly}}$, then $\Pi_2^p \subseteq \Sigma_2^p$. (coC $\subseteq$ C $\implies$ C = coC.)

Let $L \in \Pi_2^p$. Then, $\exists$ a polytime TM M such that

$$x \in L \iff \forall u_1 \exists u_2 \text{ such that } M(x, u_1, u_2) = 1$$

Define a related language L'

$$(x, u_1) \in L' \iff \exists u_2 \text{ s.t. } M(x, u_1, u_2) = 1$$

$L' \in$ NP. Let f be the function reducing L' to *SAT*.

Going back to L:

$$x \in L \iff \forall u_1\ (x, u_1) \in L' \iff \forall u_1\, f(x, u_1) \in \mathit{SAT} \iff \exists C \forall u_1\ C(f(x, u_1)) = 1$$

($\because$ *SAT* $\in$ P$_{/\text{poly}}$)

Flaw: There might be a circuit C s.t. $C(f(x, u_1)) = 1$ even if $f(x, u_1) \notin$ *SAT*.

...

Karp-Lipton Theorem

Theorem: If $\mathsf{NP} \subseteq \mathsf{P}_{/\mathsf{poly}}$, then $\mathsf{PH} = \Sigma_2^p$.

Proof:

Karp-Lipton Theorem

Theorem: If NP $\subseteq$ P$_{/\mathsf{poly}}$, then PH $= \Sigma_2^p$.

Proof: Observation: If $SAT \in$ P$_{/\mathsf{poly}}$, then a polysize circuit family $\{C_n\}$ s.t. $C_{|\phi|}(\phi)$ outputs a satisfying assignment for ϕ, if ϕ is satisfiable.

Karp-Lipton Theorem

Theorem: If NP $\subseteq$ $\mathsf{P}_{/\mathsf{poly}}$, then PH $= \Sigma_2^p$.

Proof: **Observation:** If *SAT* $\in \mathsf{P}_{/\mathsf{poly}}$, then a polysize circuit family $\{C_n\}$ s.t. $C_{|\phi|}(\phi)$ outputs a satisfying assignment for ϕ, if ϕ is satisfiable.

Continuing with plugging:

Karp-Lipton Theorem

Theorem: If NP $\subseteq$ P$_{/\mathrm{poly}}$, then PH $= \Sigma_2^p$.

Proof: Observation: If $SAT \in$ P$_{/\mathrm{poly}}$, then a polysize circuit family $\{C_n\}$ s.t. $C_{|\phi|}(\phi)$ outputs a satisfying assignment for ϕ, if ϕ is satisfiable.

Continuing with plugging:

$$x \in L \iff \forall u_1\, f(x, u_1) \in SAT$$

Karp-Lipton Theorem

Theorem: If NP $\subseteq$ P$_{/\text{poly}}$, then PH $= \Sigma_2^p$.

Proof: Observation: If $SAT \in$ P$_{/\text{poly}}$, then a polysize circuit family $\{C_n\}$ s.t. $C_{|\phi|}(\phi)$ outputs a satisfying assignment for ϕ, if ϕ is satisfiable.

Continuing with plugging:

$$x \in L \iff \forall u_1\, f(x, u_1) \in SAT$$

$$\iff \exists D \forall u_1\, D(f(x, u_1)) \text{ is a satisfying assignment for } f(x, u_1)$$

Karp-Lipton Theorem

Theorem: If NP $\subseteq$ P$_{/\text{poly}}$, then PH $= \Sigma_2^p$.

Proof: Observation: If $SAT \in$ P$_{/\text{poly}}$, then a polysize circuit family $\{C_n\}$ s.t. $C_{|\phi|}(\phi)$ outputs a satisfying assignment for ϕ, if ϕ is satisfiable.

Continuing with plugging:

Biconditional statement is true as $\exists D = C$.

$x \in L \iff \forall u_1\, f(x, u_1) \in SAT$

$\iff \exists D \forall u_1\, D(f(x, u_1))$ is a satisfying assignment for $f(x, u_1)$

Karp-Lipton Theorem

Theorem: If NP $\subseteq$ P$_{/\text{poly}}$, then PH $= \Sigma_2^p$.

Proof: Observation: If $SAT \in$ P$_{/\text{poly}}$, then a polysize circuit family $\{C_n\}$ s.t. $C_{|\phi|}(\phi)$ outputs a satisfying assignment for ϕ, if ϕ is satisfiable.

Continuing with plugging:

Biconditional statement is true as $\exists D = C$.

$$x \in L \iff \forall u_1\, f(x, u_1) \in SAT$$

$$\iff \exists D \forall u_1\, D(f(x, u_1)) \text{ is a satisfying assignment for } f(x, u_1)$$

$$\iff \exists D \forall u_1\, M(x, u_1, D) = 1$$

Karp-Lipton Theorem

Theorem: If NP $\subseteq$ P$_{/\text{poly}}$, then PH $= \Sigma_2^p$.

Proof: Observation: If $SAT \in$ P$_{/\text{poly}}$, then a polysize circuit family $\{C_n\}$ s.t. $C_{|\phi|}(\phi)$ outputs a satisfying assignment for ϕ, if ϕ is satisfiable.

Continuing with plugging:

$$x \in L \iff \forall u_1\, f(x, u_1) \in SAT$$

$$\iff \exists D \forall u_1\, D(f(x, u_1)) \text{ is a satisfying assignment for } f(x, u_1)$$

$$\iff \exists D \forall u_1\, M(x, u_1, D) = 1$$

Biconditional statement is true as $\exists D = C$.

M outputs 1 iff $D(f(x, u_1))$ is a satisfying assignment for $f(x, u_1)$.

Karp-Lipton Theorem

Theorem: If NP $\subseteq$ $\mathsf{P}_{/\mathsf{poly}}$, then PH $= \Sigma_2^p$.

Proof: Observation: If $SAT \in \mathsf{P}_{/\mathsf{poly}}$, then a polysize circuit family $\{C_n\}$ s.t. $C_{|\phi|}(\phi)$ outputs a satisfying assignment for ϕ, if ϕ is satisfiable.

Continuing with plugging:

Biconditional statement is true as $\exists D = C$.

$$x \in L \iff \forall u_1\, f(x, u_1) \in SAT$$

$$\iff \exists D \forall u_1\, D(f(x, u_1)) \text{ is a satisfying assignment for } f(x, u_1)$$

$$\iff \exists D \forall u_1\, M(x, u_1, D) = 1$$

M outputs 1 iff $D(f(x, u_1))$ is a satisfying assignment for $f(x, u_1)$.

Thus, $L \in \Sigma_2^p$.

Karp-Lipton Theorem

Theorem: If NP $\subseteq$ P$_{/\text{poly}}$, then PH $= \Sigma_2^p$.

Proof: **Observation:** If *SAT* $\in$ P$_{/\text{poly}}$, then a polysize circuit family $\{C_n\}$ s.t. $C_{|\phi|}(\phi)$ outputs a satisfying assignment for ϕ, if ϕ is satisfiable.

Continuing with plugging:

$$x \in L \iff \forall u_1\, f(x, u_1) \in SAT$$

$$\iff \exists D \forall u_1\, D(f(x, u_1)) \text{ is a satisfying assignment for } f(x, u_1)$$

$$\iff \exists D \forall u_1\, M(x, u_1, D) = 1$$

Biconditional statement is true as $\exists D = C$.

M outputs 1 iff $D(f(x, u_1))$ is a satisfying assignment for $f(x, u_1)$.

Thus, $L \in \Sigma_2^p$. ■