CS310 Automata Theory – 2016-2017

Nutan Limaye

Lecture 33: Effective computation April 06, 2017

Turing machines with resource constraints.

Turing machines with resource constraints.

Resources for computation.

Turing machines with resource constraints.

Resources for computation.

Time

Turing machines with resource constraints.

Resources for computation.

Time: the number steps for which the TM runs

Turing machines with resource constraints.

Resources for computation.

Time: the number steps for which the TM runs Space

Turing machines with resource constraints.

Resources for computation.

Time: the number steps for which the TM runs

Space: the number of different cells on which the TM writes

Turing machines with resource constraints.

Resources for computation.

Time: the number steps for which the TM runs

Space: the number of different cells on which the TM writes

The number of times an input bit can be read

Turing machines with resource constraints.

Resources for computation.

Time: the number steps for which the TM runs

Space: the number of different cells on which the TM writes

The number of times an input bit can be read

The amount of energy used

Turing machines with resource constraints.

Resources for computation.

Time: the number steps for which the TM runs Space: the number of different cells on which the TM writes The number of times an input bit can be read

The amount of energy used

:

Turing machines with resource constraints.

Resources for computation.

Time: the number steps for which the TM runs Space: the number of different cells on which the TM writes The number of times an input bit can be read The amount of energy used :

Why bound resorces?

Viewing TM as algorithms.

Turing machines with resource constraints.

Resources for computation.

Time: the number steps for which the TM runs Space: the number of different cells on which the TM writes The number of times an input bit can be read The amount of energy used:

Why bound resorces?

Viewing TM as algorithms.

TM to help in computation of important problems.

Turing machines with resource constraints.

Resources for computation.

Time: the number steps for which the TM runs Space: the number of different cells on which the TM writes

The number of times an input bit can be read

The amount of energy used

:

Why bound resorces?

Viewing TM as algorithms.

TM to help in computation of important problems.

Finer study of decidable languages.

Turing machines with resource constraints.

Resources for computation.

Time: the number steps for which the TM runs Space: the number of different cells on which the TM writes

The number of times an input bit can be read

The amount of energy used

:

Why bound resorces?

Viewing TM as algorithms.

TM to help in computation of important problems.

Finer study of decidable languages.

How should we bound the resources?

Turing machines with resource constraints.

Resources for computation.

Time: the number steps for which the TM runs

Space: the number of different cells on which the TM writes

The number of times an input bit can be read

The amount of energy used

:

Why bound resorces?

Viewing TM as algorithms.

TM to help in computation of important problems.

Finer study of decidable languages.

How should we bound the resources?

Many different ways exist. ...



Let $t: \mathbb{N} \to \mathbb{N}$.

Let $t: \mathbb{N} \to \mathbb{N}$.

Definition

A language $L \subseteq \Sigma^*$ is said to be in class TIME(t(n))

Let $t: \mathbb{N} \to \mathbb{N}$.

Definition

A language $L \subseteq \Sigma^*$ is said to be in class TIME(t(n)) if there exists a deterministic Turing machine M such that $\forall x \in \Sigma^*$,

Let $t: \mathbb{N} \to \mathbb{N}$.

Definition

A language $L \subseteq \Sigma^*$ is said to be in class TIME(t(n)) if there exists a deterministic Turing machine M such that $\forall x \in \Sigma^*$,

M halts on x in time O(t(|x|)), where |x| indicates the length of x.

Let $t: \mathbb{N} \to \mathbb{N}$.

Definition

A language $L \subseteq \Sigma^*$ is said to be in class TIME(t(n)) if there exists a deterministic Turing machine M such that $\forall x \in \Sigma^*$,

M halts on x in time O(t(|x|)), where |x| indicates the length of x. if $x \in L$ then M accepts x.

Let $t: \mathbb{N} \to \mathbb{N}$.

Definition

A language $L \subseteq \Sigma^*$ is said to be in class TIME(t(n)) if there exists a deterministic Turing machine M such that $\forall x \in \Sigma^*$,

M halts on x in time O(t(|x|)), where |x| indicates the length of x.

if $x \in L$ then M accepts x.

if $x \notin L$ then M rejects x.

Let $t: \mathbb{N} \to \mathbb{N}$.

Definition

A language $L \subseteq \Sigma^*$ is said to be in class TIME(t(n)) if there exists a deterministic Turing machine M such that $\forall x \in \Sigma^*$,

M halts on x in time O(t(|x|)), where |x| indicates the length of x. if $x \in L$ then M accepts x.

if $x \notin L$ then M rejects x.

$$P = \bigcup_{k} \mathsf{TIME}(n^k)$$

Let $t: \mathbb{N} \to \mathbb{N}$.

Definition

A language $L \subseteq \Sigma^*$ is said to be in class TIME(t(n)) if there exists a deterministic Turing machine M such that $\forall x \in \Sigma^*$,

M halts on x in time O(t(|x|)), where |x| indicates the length of x. if $x \in L$ then M accepts x.

if $x \notin L$ then M rejects x.

$$P = \bigcup_k \mathsf{TIME}(n^k)$$

$$EXP = \bigcup_{k} TIME(2^{n^k})$$



Let $t: \mathbb{N} \to \mathbb{N}$.

Let $t: \mathbb{N} \to \mathbb{N}$.

Definition

A language $L \subseteq \Sigma^*$ is said to be in class NTIME(t(n))

Let $t: \mathbb{N} \to \mathbb{N}$.

Definition

A language $L \subseteq \Sigma^*$ is said to be in class $\mathsf{NTIME}(t(n))$ if there exists a non-deterministic Turing machine M such that $\forall x \in \Sigma^*$,

Let $t: \mathbb{N} \to \mathbb{N}$.

Definition

A language $L \subseteq \Sigma^*$ is said to be in class $\mathsf{NTIME}(t(n))$ if there exists a non-deterministic Turing machine M such that $\forall x \in \Sigma^*$,

each run of M halts on x in time O(t(|x|)), where |x| indicates the length of x.

Let $t: \mathbb{N} \to \mathbb{N}$.

Definition

A language $L \subseteq \Sigma^*$ is said to be in class $\mathsf{NTIME}(t(n))$ if there exists a non-deterministic Turing machine M such that $\forall x \in \Sigma^*$,

each run of M halts on x in time O(t(|x|)), where |x| indicates the length of x.

if $x \in L$ then

Let $t: \mathbb{N} \to \mathbb{N}$.

Definition

A language $L \subseteq \Sigma^*$ is said to be in class $\mathsf{NTIME}(t(n))$ if there exists a non-deterministic Turing machine M such that $\forall x \in \Sigma^*$,

each run of M halts on x in time O(t(|x|)), where |x| indicates the length of x.

if $x \in L$ then M accepts x on at least one run.

Let $t: \mathbb{N} \to \mathbb{N}$.

Definition

A language $L \subseteq \Sigma^*$ is said to be in class $\mathsf{NTIME}(t(n))$ if there exists a non-deterministic Turing machine M such that $\forall x \in \Sigma^*$,

each run of M halts on x in time O(t(|x|)), where |x| indicates the length of x.

if $x \in L$ then M accepts x on at least one run.

if $x \notin L$ then

Let $t: \mathbb{N} \to \mathbb{N}$.

Definition

A language $L \subseteq \Sigma^*$ is said to be in class $\mathsf{NTIME}(t(n))$ if there exists a non-deterministic Turing machine M such that $\forall x \in \Sigma^*$,

each run of M halts on x in time O(t(|x|)), where |x| indicates the length of x.

if $x \in L$ then M accepts x on at least one run.

if $x \notin L$ then M rejects x on all runs.

Let $t: \mathbb{N} \to \mathbb{N}$.

Definition

A language $L \subseteq \Sigma^*$ is said to be in class $\mathsf{NTIME}(t(n))$ if there exists a non-deterministic Turing machine M such that $\forall x \in \Sigma^*$,

each run of M halts on x in time O(t(|x|)), where |x| indicates the length of x.

if $x \in L$ then M accepts x on at least one run.

if $x \notin L$ then M rejects x on all runs.

$$NP = \bigcup_{k} \mathsf{NTIME}(n^k)$$

Let $t: \mathbb{N} \to \mathbb{N}$.

Definition

A language $L \subseteq \Sigma^*$ is said to be in class $\mathsf{NTIME}(t(n))$ if there exists a non-deterministic Turing machine M such that $\forall x \in \Sigma^*$,

each run of M halts on x in time O(t(|x|)), where |x| indicates the length of x.

if $x \in L$ then M accepts x on at least one run.

if $x \notin L$ then M rejects x on all runs.

$$NP = \bigcup_{k} NTIME(n^{k})$$

$$NEXP = \bigcup_{k} NTIME(2^{n^{k}})$$

Relationships between models

Lemma

Let t(n) > n. Let L be a language decided by a multitape TM in time t(n).

Relationships between models

Lemma

Let t(n) > n. Let L be a language decided by a multitape TM in time t(n). Then there is a single tape TM that decides L in time

Relationships between models

Lemma

Let t(n) > n. Let L be a language decided by a multitape TM in time t(n). Then there is a single tape TM that decides L in time $O((t(n))^2)$.

Lemma

Let t(n) > n. Let L be a language decided by a multitape TM in time t(n). Then there is a single tape TM that decides L in time $O((t(n))^2)$.

Proof idea:

Lemma

Let t(n) > n. Let L be a language decided by a multitape TM in time t(n). Then there is a single tape TM that decides L in time $O((t(n))^2)$.

Proof idea:

East step of multitape machine can be executed on a single tape machine in time O(t(n)).

Lemma

Let t(n) > n. Let L be a language decided by a multitape TM in time t(n). Then there is a single tape TM that decides L in time $O((t(n))^2)$.

Proof idea:

East step of multitape machine can be executed on a single tape machine in time O(t(n)).

Lemma

Let t(n) > n. Let L be a language decided by a non-deterministic TM in time t(n).

Lemma

Let t(n) > n. Let L be a language decided by a multitape TM in time t(n). Then there is a single tape TM that decides L in time $O((t(n))^2)$.

Proof idea:

East step of multitape machine can be executed on a single tape machine in time O(t(n)).

Lemma

Let t(n) > n. Let L be a language decided by a non-deterministic TM in time t(n). Then there is a deterministic TM that decides L in time

Lemma

Let t(n) > n. Let L be a language decided by a multitape TM in time t(n). Then there is a single tape TM that decides L in time $O((t(n))^2)$.

Proof idea:

East step of multitape machine can be executed on a single tape machine in time O(t(n)).

Lemma

Let t(n) > n. Let L be a language decided by a non-deterministic TM in time t(n). Then there is a deterministic TM that decides L in time $2^{O(t(n))}$.

Lemma

Let t(n) > n. Let L be a language decided by a multitape TM in time t(n). Then there is a single tape TM that decides L in time $O((t(n))^2)$.

Proof idea:

East step of multitape machine can be executed on a single tape machine in time O(t(n)).

Lemma

Let t(n) > n. Let L be a language decided by a non-deterministic TM in time t(n). Then there is a deterministic TM that decides L in time $2^{O(t(n))}$.

Proof idea:

Lemma

Let t(n) > n. Let L be a language decided by a multitape TM in time t(n). Then there is a single tape TM that decides L in time $O((t(n))^2)$.

Proof idea:

East step of multitape machine can be executed on a single tape machine in time O(t(n)).

Lemma

Let t(n) > n. Let L be a language decided by a non-deterministic TM in time t(n). Then there is a deterministic TM that decides L in time $2^{O(t(n))}$.

Proof idea: DIY

How are P, NP, EXP, and NEXP related?

How are P, NP, EXP, and NEXP related? $P \subseteq NP$ by definition.

How are P, NP, EXP, and NEXP related?

 $P \subseteq NP$ by definition.

 $P \subseteq EXP$ again by definition.

How are P, NP, EXP, and NEXP related?

 $P \subseteq NP$ by definition.

 $P \subseteq EXP$ again by definition.

Similarly, $NP \subseteq NEXP$ by definition.

How are P, NP, EXP, and NEXP related?

 $P \subseteq NP$ by definition.

 $P \subseteq EXP$ again by definition.

Similarly, $NP \subseteq NEXP$ by definition.

How are P, NP, EXP, and NEXP related?

 $P \subseteq NP$ by definition.

 $P \subseteq EXP$ again by definition.

Similarly, $NP \subseteq NEXP$ by definition.

Finally, $NP \subseteq EXP$ due to the previous lemma.

 $\mathsf{P} \longrightarrow \mathsf{NP}$

EXP

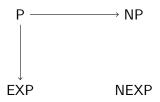
NEXP

How are P, NP, EXP, and NEXP related?

 $P \subseteq NP$ by definition.

 $P \subseteq EXP$ again by definition.

Similarly, $NP \subseteq NEXP$ by definition.

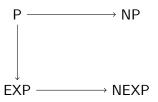


How are P, NP, EXP, and NEXP related?

 $P \subseteq NP$ by definition.

 $P \subseteq EXP$ again by definition.

Similarly, $NP \subseteq NEXP$ by definition.

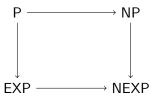


How are P, NP, EXP, and NEXP related?

 $P \subseteq NP$ by definition.

 $P \subseteq EXP$ again by definition.

Similarly, $NP \subseteq NEXP$ by definition.

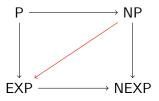


How are P, NP, EXP, and NEXP related?

 $P \subseteq NP$ by definition.

 $P \subseteq EXP$ again by definition.

Similarly, $NP \subseteq NEXP$ by definition.

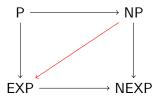


How are P, NP, EXP, and NEXP related?

 $P \subseteq NP$ by definition.

 $P \subseteq EXP$ again by definition.

Similarly, $NP \subseteq NEXP$ by definition.



P vs. NP

P vs. NP

P the class of languages where membership can be decided quickly.

P vs. NP

P the class of languages where membership can be decided quickly.

NP the class of languages where membership can be verified quickly.

 $\mathsf{SAT} = \{ \phi \, | \, \phi \text{ is satisfiable} \}.$

SAT = $\{\phi \mid \phi \text{ is satisfiable}\}$. in NP (and not known to be in P)

SAT = $\{\phi \mid \phi \text{ is satisfiable}\}$. in NP (and not known to be in P)

Reach = $\{(G, s, t) \mid t \text{ is reachable from } s \text{ in } G\}$.

SAT = $\{\phi \mid \phi \text{ is satisfiable}\}$. in NP (and not known to be in P)

Reach = $\{(G, s, t) | t \text{ is reachable from } s \text{ in } G\}$. in P

SAT =
$$\{\phi \mid \phi \text{ is satisfiable}\}$$
. in NP (and not known to be in P)

Reach =
$$\{(G, s, t) \mid t \text{ is reachable from } s \text{ in } G\}$$
. in P

3-SAT =
$$\{\phi \mid \phi \text{ is a 3-CNF and satisfiable}\}.$$

SAT = $\{\phi \mid \phi \text{ is satisfiable}\}$. in NP (and not known to be in P)

Reach = $\{(G, s, t) \mid t \text{ is reachable from } s \text{ in } G\}$. in P

3-SAT = $\{\phi \mid \phi \text{ is a 3-CNF and satisfiable}\}$. in NP (and not known to be in P)

SAT = $\{\phi \mid \phi \text{ is satisfiable}\}$. in NP (and not known to be in P)

Reach = $\{(G, s, t) \mid t \text{ is reachable from } s \text{ in } G\}$. in P

3-SAT = $\{\phi \mid \phi \text{ is a 3-CNF and satisfiable}\}$. in NP (and not known to be in P)

2-SAT = $\{\phi \mid \phi \text{ is a 2-CNF and satisfiable}\}.$

SAT =
$$\{\phi \mid \phi \text{ is satisfiable}\}$$
. in NP (and not known to be in P)

Reach =
$$\{(G, s, t) \mid t \text{ is reachable from } s \text{ in } G\}$$
. in P

3-SAT =
$$\{\phi \mid \phi \text{ is a 3-CNF and satisfiable}\}$$
. in NP (and not known to be in P)

2-SAT =
$$\{\phi \mid \phi \text{ is a 2-CNF and satisfiable}\}$$
. in P

SAT =
$$\{\phi \mid \phi \text{ is satisfiable}\}$$
. in NP (and not known to be in P)

Reach = $\{(G, s, t) \mid t \text{ is reachable from } s \text{ in } G\}$. in P

3-SAT = $\{\phi \mid \phi \text{ is a 3-CNF and satisfiable}\}$. in NP (and not known to be in P)

2-SAT = $\{\phi \mid \phi \text{ is a 2-CNF and satisfiable}\}$. in P

Factoring = $\{(k, n) \mid n \text{ has a factor } \leq k\}$.

SAT =
$$\{\phi \mid \phi \text{ is satisfiable}\}$$
. in NP (and not known to be in P)

Reach =
$$\{(G, s, t) | t \text{ is reachable from } s \text{ in } G\}$$
. in P

3-SAT =
$$\{\phi \mid \phi \text{ is a 3-CNF and satisfiable}\}$$
. in NP (and not known to be in P)

2-SAT =
$$\{\phi \mid \phi \text{ is a 2-CNF and satisfiable}\}$$
. in P

Factoring =
$$\{(k, n) \mid n \text{ has a factor } \leq k\}$$
. Google it!

SAT =
$$\{\phi \mid \phi \text{ is satisfiable}\}$$
. in NP (and not known to be in P)

Reach =
$$\{(G, s, t) \mid t \text{ is reachable from } s \text{ in } G\}$$
. in P

3-SAT =
$$\{\phi \mid \phi \text{ is a 3-CNF and satisfiable}\}$$
. in NP (and not known to be in P)

$$2\text{-SAT} = \{\phi \mid \phi \text{ is a 2-CNF and satisfiable}\}.$$
 in P

Factoring =
$$\{(k, n) \mid n \text{ has a factor } \leq k\}$$
. Google it!

Clique =
$$\{(G, k) \mid G \text{ has a clique of size } \geq k\}$$
.



SAT =
$$\{\phi \mid \phi \text{ is satisfiable}\}$$
. in NP (and not known to be in P)

Reach =
$$\{(G, s, t) | t \text{ is reachable from } s \text{ in } G\}$$
. in P

3-SAT =
$$\{\phi \mid \phi \text{ is a 3-CNF and satisfiable}\}$$
. in NP (and not known to be in P)

2-SAT =
$$\{\phi \mid \phi \text{ is a 2-CNF and satisfiable}\}$$
. in P

Factoring =
$$\{(k, n) \mid n \text{ has a factor } \leq k\}$$
. Google it!

Clique = $\{(G, k) \mid G \text{ has a clique of size } \geq k\}$. in NP (and not known to be in P)



SAT =
$$\{\phi \mid \phi \text{ is satisfiable}\}$$
. in NP (and not known to be in P)

Reach =
$$\{(G, s, t) | t \text{ is reachable from } s \text{ in } G\}$$
. in P

3-SAT =
$$\{\phi \mid \phi \text{ is a 3-CNF and satisfiable}\}$$
. in NP (and not known to be in P)

2-SAT =
$$\{\phi \mid \phi \text{ is a 2-CNF and satisfiable}\}$$
. in P

Factoring =
$$\{(k, n) \mid n \text{ has a factor } \leq k\}$$
. Google it!

Clique = $\{(G, k) \mid G \text{ has a clique of size } \geq k\}$. in NP (and not known to be in P)



Time heirarchy theorem

How do we separate NP from P?

Time heirarchy theorem

How do we separate NP from P?

To prove

Method used

How do we separate NP from P?

To prove

Method used

not regular

How do we separate NP from P?

To prove Method used

not regular pumping lemma for REG

How do we separate NP from P?

To prove Method used

not regular pumping lemma for REG

non-context-free

How do we separate NP from P?

To prove Method used

not regular pumping lemma for REG

non-context-free pumping lemma or CFLs

How do we separate NP from P?

To prove Method used

not regular pumping lemma for REG

non-context-free pumping lemma or CFLs

not recognizable

How do we separate NP from P?

To prove Method used

not regular pumping lemma for REG

non-context-free pumping lemma or CFLs

not recognizable diagonalization

How do we separate NP from P?

To prove Method used

not regular pumping lemma for REG

non-context-free pumping lemma or CFLs

not recognizable diagonalization

not decidable

How do we separate NP from P?

To prove Method used

not regular pumping lemma for REG

non-context-free pumping lemma or CFLs

not recognizable diagonalization

not decidable Rice's theorem

How do we separate NP from P?

To prove Method used

not regular pumping lemma for REG

non-context-free pumping lemma or CFLs

not recognizable diagonalization

not decidable Rice's theorem or diagonalization and reductions

How do we separate NP from P?

To prove Method used

not regular pumping lemma for REG

non-context-free pumping lemma or CFLs

not recognizable diagonalization

not decidable Rice's theorem or diagonalization and reductions

not in P

How do we separate NP from P?

To prove Method used

not regular pumping lemma for REG

non-context-free pumping lemma or CFLs

not recognizable diagonalization

not decidable Rice's theorem or diagonalization and reductions

not in P ????

Definition

A function $t: \mathbb{N} \to \mathbb{N}$ is said to be time constructible

Definition

A function $t: \mathbb{N} \to \mathbb{N}$ is said to be time constructible if the there exists a TM that on input 1^n , it outputs t(n) in time O(t(n)).

Definition

A function $t: \mathbb{N} \to \mathbb{N}$ is said to be time constructible if the there exists a TM that on input 1^n , it outputs t(n) in time O(t(n)).

Examples

Definition

A function $t: \mathbb{N} \to \mathbb{N}$ is said to be time constructible if the there exists a TM that on input 1^n , it outputs t(n) in time O(t(n)).

Examples

 n^2

Definition

A function $t: \mathbb{N} \to \mathbb{N}$ is said to be time constructible if the there exists a TM that on input 1^n , it outputs t(n) in time O(t(n)).

Examples

 n^2 , $n \log n$.

Definition

A function $t: \mathbb{N} \to \mathbb{N}$ is said to be time constructible if the there exists a TM that on input 1^n , it outputs t(n) in time O(t(n)).

Examples

 n^2 , $n \log n$.

Theorem

Let $t : \mathbb{N} \to \mathbb{N}$ be a time constructible function. There exists a language L such that $L \in TIME(t(n)^2)$, but $L \notin TIME(o(t(n)))$.

Definition

A function $t: \mathbb{N} \to \mathbb{N}$ is said to be time constructible if the there exists a TM that on input 1^n , it outputs t(n) in time O(t(n)).

Examples

 n^2 , $n \log n$.

Theorem

Let $t : \mathbb{N} \to \mathbb{N}$ be a time constructible function. There exists a language L such that $L \in TIME(t(n)^2)$, but $L \notin TIME(o(t(n)))$.