Michael A. Forbes
MForbes@illinois.edu
2023-08-28.1

cs579 Computational Complexity - Lecture 3 (2023-08-29)

logistics: pset 1 due 09-07
W 10:30 - 12:30
Zander office hrs Siebel 3303

last lecture. time complexity - def [# steps, worst case wrt input]
- examples [$O(n^2)$, $n\log n$, n; 1 tape, 1 tape, 2 tape]
- robustness [2 tape vs 1 tape] [model indep]

today: non-determinism
[move to front] [Lapages]

def. PATH = $\{ \langle G, s, t \rangle : G = (V, E)$ directed, $s, t \in V$, G has $s \rightsquigarrow t$ path$\}$
← any [reasonable] encoding into Σ^* [alphabet] [adj matrix, list] [encoding index results]
← efficiently transformable into other encodings

prop: PATH $\in$ P [poly-time algo, worst case]
[374]
sketch: depth-first search

def: HAMPATH = $\{ \langle G, s, t \rangle : G$ has $s \rightsquigarrow t$ path visiting each vertex [exactly] once$\}$
↳ Hamiltonian path
Q: HAMPATH $\in$ P? [Q] [open]
A: [no] answer [not real]

"algo": "on input $\langle G = (V, E), s, t \rangle$:
- for $V = \{v_1, \dots, v_n\}$ [guess] $v_{i_1}, \dots, v_{i_n} \in V$, $n = |V|$ [abuse convention]
- [check]
  - reject if repeated vertex
  - reject if $v_{i_1} \neq s$, $v_{i_n} \neq t$ or $(v_{i_j}, v_{i_{j+1}}) \notin E$ some j
  - accept

poly-time
n^n

correctness: clear
complexity: [if] guess is ham-path, then efficient
n^n guesses

goal: model "guessing" as a computational resource [non] determinism [not] realistic, [is] useful to characterize problems

2023.08.29.1
def: nondeterministic Turing machine (NTM) is a TM with transition function $\delta : Q \times \Gamma \to 2^{Q \times \Gamma \times \{L, S, R\}}$
[state] [tape read] [power set] [new state] [move] [write]
[set] of possible transitions
[guess] within set
δ:
- [then halt] acc
- [then halt] rej
- or dies, $\delta(-) = \emptyset$ [no valid transitions]
- loops [no halting]

[> 2 choices]

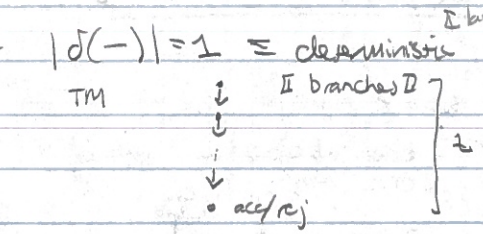
Branch is sequence of valid transitions.
Branch accepts input x if sequence reaches acc
— " — rejects — " —

NTM N accepts input x if [some] branch of N on x accepts
— " — rejects — " — [all] — " — rejects
[halts vs not]

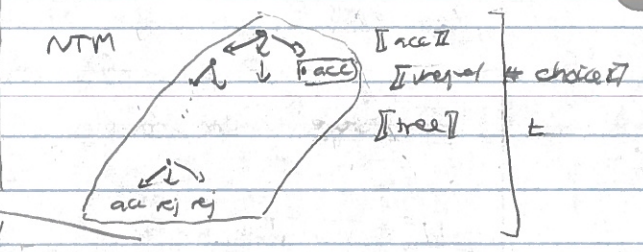
time of N on x is length of longest branch [other measures possible, this is reasonable]

Michael A. Forbes
MiForbes@illinois.edu
2023-08-24.2

eg - $|\delta(-)| = 1 \equiv$ deterministic [[bit basis]]



,



def: NTM N runs in time $t(n): \mathbb{N} \to \mathbb{N}$ if
for all $x \in \Sigma^n$ N acc/rej in $\leq t(n)$ steps [[on all branches]]
$NTIME(t(n)) = \{ L : L = L(N)$ [[accepted inputs]], N runs in time $O(t(n)) \}$
$NP = \bigcup_k NTIME(n^k)$ [[nondeterministic polynomial time]]

lem: $P \subseteq NP$ [[use single transition]]
[[1-tape vs 2-tape]]
rmk: NP is model invariant

- foer

Q: what is in NP?

prop: HAMPATH $\in NP$

pf: idea: use many branches to try all possible paths

alg: $N =$ "on input $\langle G=(V,E), s, t \rangle$ [[$n = |V|$]]
- for $V = \{v_1, \dots, v_n\}$, nondeterministically write down $v_1, \dots, v_n \in V$
  eg: $\delta(q,\gamma) \mapsto \{(q',0,R),(q',1,R)\}$ guesses 1 bit [[goes to tape]]
  $\Rightarrow$ guessing $\leq \lg n$ bits produces $v \in V$
  $\Rightarrow$ guessing $\leq n \lg n$ bits produces
- accept if $v_{i_1} \to v_{i_2} \to \cdots \to v_{i_n}$ is a valid $s \rightsquigarrow t$ hampath"
  ($v_{i_1} = s$, $v_{i_n} = t$)

correctness: clear [[same alg as above]]

complexity: each branch is poly(n) steps [[but many branches]]

[[another view]]
def: verifier for language L is TM V w/
$L = \{ x : V$ accepts $\langle x, w \rangle$ [[encoding]], some $w \in \Sigma^*$ [[witness]] $\}$
V runs in time $t(n): \mathbb{N} \to \mathbb{N}$ if for all $x \in \Sigma^n$,
$x \in L$ iff V accepts $\langle x, w \rangle$ for some $w \in \Sigma^*$ in $\leq t(n)$ steps
$\Rightarrow |w| \leq t(n)$. [[can only read that much]]

encoding specific

prop: $L \in NP$ iff L has polytime verifier

pf: $\Rightarrow$: NTM N acc L in $\leq t(n)$ steps
$A = \{ \langle x, w \rangle : w$ is description of accepting branch [[sequence of transitions]] $\}$
$\Rightarrow x \in L$ iff $|w| \leq O(t(n))$ exists
↪ each transition takes $O(1)$ bits to describe
and checking if w is "clearly" efficient [[simulate N]]

correctness/complexity

Michael A. Forbes
MForbes.illinois.edu
2023-08-24 <3

$\Leftarrow$: V $t(n)$-time verifier for L

N = "on input x:
- guess $w \in \Sigma^*$ of length $\leq t(n)$
- accept iff V accepts $\langle x, w \rangle$"

correctness, complexity = "clear" ∎

rmk: both view points useful

Q: P vs NP ?

prop: $t(n): \mathbb{N} \to \mathbb{N}$. $TIME(t(n)) \subseteq NTIME(t(n)) \subseteq TIME(2^{O(t(n))})$

pf: (1): clear [single transition (1) gadget] [NTM as exercise] time construction

(2): verifier version

V $t(n)$ time verifier for L

M = "on input x:
- for all $w \in \Sigma^{\leq t(n)}$ [$|\Sigma^{O(t(n))}| = 2^{O(t(n))}$, $|O(t(n))|$]
- check if V accepts $\langle x, w \rangle$
- accept if V ever accepts"

correctness: clear

complexity: $poly(t, 2^{O(t)}) = 2^{O(t)}$ [exp] [gen] ∎

Q: $\overline{HAMPATH} = \Sigma^* \setminus HAMPATH \in NP$?

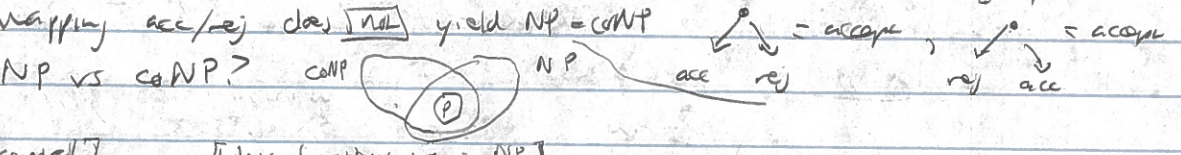
def: $noHAMPATH = \{\langle G, s, t \rangle : G$ has [no] $s \to t$ hampath$\}$ [unclear how to verify] [facts] [negation]

lem: $\overline{HAMPATH} \simeq noHAMPATH$ by handling improper encoding / [not $\langle G, s, t \rangle$] [can formalize via next lecture]

def: $coNP = \{\overline{L} : L \in NP\}$ [complement]

lem: $coP = \{\overline{L} : L \in P\} = P$ [swap acc/rej]

rmk: swapping acc/rej does [not] yield $NP = coNP$



Q: P vs NP vs coNP?

conj: [central] $P = NP$ [lots of problems are in NP] [recognition easier than creation (music, proofs)] [hard! [many] clear also, need to rule [all] out]

eg: $PRIMES = \{\langle n \rangle : n$ is prime integer$\}$

↑ [binary] encoding, length $O(\lg n)$

n prime iff [no] nontrivial factorization $n = a \cdot b$, $a, b < n$

$\to$ $PRIMES \in TIME(poly(n))$ [brute force] [not] efficient

n [not] prime iff [exists] "

$\Rightarrow$ $PRIMES \in NTIME(poly(\lg n))$ [efficient]

$\Rightarrow$ $\overline{PRIMES} \in coNP$

N = "on input $\langle n \rangle$:
- guess $a, b < n$
- accept iff $n = a \cdot b$"

Michael A. Forbes
M.forbes@illinois.edu
2023-08-23.4

Q: do better?

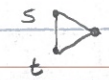
thm [Pratt 75]: PRIMES ∈ NP ∩ coNP [elem number theory]

thm [Agrawal Kayal Saxena 02]: PRIMES ∈ P [many intermediate work] [took a while] [established "evidence" ∈ P] [non elem number theory]

[more recent] [another example]

def: $G = (V, E)$ undirected, $s \neq t \in V$.

$s \rightsquigarrow t$ path is Eulerian if all edges are used exactly [once]. [can repeat vertices]

eg:  no eulerian path,  eulerian

def: EULERPATH = $\{\langle G, s, t\rangle$: G undirected [connected] [no euler path if unconnected] w/ $s \rightsquigarrow t$ eulerian path$\}$ [as in hampath]

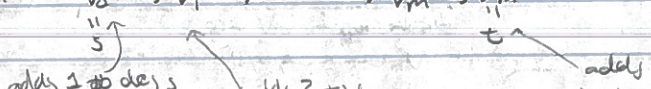
prop: ——— ∈ NP

prop: G connected, $s \neq t$

G has $s \rightsquigarrow t$ eulerian path iff
- $\deg s$, $\deg t$ odd [# incident edges]
- $v \neq s, t$, $\deg v$ even

[efficiently checkable] [non obvious!]

cor: EULERPATH ∈ P

sketch $\Rightarrow$: 

$$\deg_v v := \deg_p v = \begin{cases} 2\,(\#\text{occur of } v \text{ in } p) & v \neq s, t \quad [\text{even}] \\ \text{——} - 1 & v = s, t \quad [\text{odd}] \end{cases}$$

(p euler [increasing direction] [edge counted])

sketch $\Leftarrow$: exercise

[not realistic] [models guessing]

today: nondeterministic TMs [verifier view]

NTIME, NP [longest path]

HAMPATH [in NP, open if in P] [clever algo - primes - euler path]

next lecture: NP completeness

logistics: pset 1 due 09-07

Zander office hours: W 10:30-12:30, Siebel 3303