

Algoritmuselmélet 14. előadás

Katona Gyula Y.
Budapesti Műszaki és Gazdaságtudományi Egyetem
Számítástudományi Tsz.
I. B. 137/b
kiskat@cs.bme.hu

2002 Április 22.

Idő- és tárkorlátok

Definíció. Legyen $t : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ egy függvény, melyre minden $n \in \mathbb{Z}^+$ esetén $t(n) \geq n$ teljesül. Az M Turing-gép $t(n)$ **időkorlátos**, ha n hosszú inputokon legfeljebb $t(n)$ lépést tesz (más szóval $T_M(n) \leq t(n)$).

$t(n) \geq n \implies$ a gép legalább végigolvashatja az inputot
 M gyors $\implies t(n)$ lassan növekedő függvény

Példa: hárommal való oszthatóságot ellenőrző Turing-gép $\implies n + 1$
 időkorlátos

Definíció.

$$TIME(t(n)) := \left\{ L \subseteq I^* \mid \begin{array}{l} L \text{ felismerhető egy } O(t(n)) \text{ időkorlátos} \\ M \text{ Turing-géppel} \end{array} \right\}.$$

$TIME(t(n)) \implies$ létezik $ct(n)$ időkorlátos TG
 n hosszú x inputokon a számítás **mindig befejeződik** legfeljebb $ct(n)$
 lépésben, tekintet nélkül arra, hogy $x \in L$ igaz-e
 $\implies TIME(t(n)) \subset \mathcal{R}$

Példa: $TIME(n) = \{\text{az } O(n), \text{ azaz lineáris időben felismerhető nyelvek}\}.$

A P nyelvosztály

Definíció. $P = \cup_{k \geq 1} TIME(n^k)$, a polinom időben felismerhető nyelvek osztálya.

Tétel. Ha az L nyelv $n^{\log n}$ -nél rövidebb időben nem ismerhető fel, akkor $L \notin P$.

Bizonyítás: Indirekt tegyük fel, hogy $L \in P$. \implies van olyan $k > 0$, melyre $L \in TIME(n^k) \implies n^{\log n} \leq cn^k$ teljesülne végtelen sok n -re ⚡

Tárkorlát

Definíció. Legyen $s : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ olyan függvény, melyre minden $n \in \mathbb{Z}^+$ számmal igaz, hogy $s(n) \geq \log_2 n$. Az M Turing-gép $s(n)$ **tárkorlátos**, ha n hosszú inputokon legfeljebb $s(n)$ tárcellát használ a **munkaszalagokon** (azaz $S_M(n) \leq s(n)$).

$s(n) \geq \log_2 n \implies$ Ennyi hely kell ahhoz, hogy egy n cellából álló szalagrészt címezni tudjunk.

Definíció.

$$SPACE(s(n)) := \left\{ L \subseteq I^* \mid \begin{array}{l} \text{az } L \text{ felismerhető egy } O(s(n)) \\ \text{tárkorlátos } M \text{ Turing-géppel} \end{array} \right\}.$$

Ez nem biztos, hogy egyáltalán megáll!

Példa: $SPACE(\log n)$ a **logaritmikus tárban felismerhető nyelvek** osztálya.

Függvényosztályok

Definíció. $FTIME(t(n)) :=$ az $O(t(n))$ időkorlátos TG-k által kiszámítható $f : I^* \rightarrow I^*$ függvények osztálya.

Definíció. $FSPACE(s(n)) :=$ az $O(s(n))$ tárkorlátos TG-k által kiszámítható $f : I^* \rightarrow I^*$ (parciális) függvények osztálya.

Definíció. $FP := \cup_{k \geq 1} FTIME(n^k)$.

Tár–idő-tétel

Tétel. [tár–idő-tétel] Ha $L \in SPACE(s(n))$, akkor van olyan L -től függő c konstans, mellyel $L \in TIME(c^{s(n)})$ teljesül.

Bizonyítás: Legyen M egy $S(n) = c_1 s(n)$ tárkorlátos ($c_1 \geq 1$) k -szalagos TG, mely felismeri L -et \implies konstruálunk olyan $O(c^{S(n)})$ -időkorlátos N TG-t, melynek a nyelve szintén L .

a gép egy pillanatnyi helyzete \implies az input, a munkaszalagok tartalma, a gép aktuális belső állapota, valamint a fejek helyzete \implies PHL

kétszer ugyanaz a PHL \implies utána ugyanaz fog történni \implies végtelen ciklus

Belátjuk, hogy ha M tárkorlátos \implies véges sok PHL lehet \implies biztos végtelen ciklusba fog kerülni (ha nem áll meg)

Ezt kellene felismerni $O(c^{S(n)})$ idő alatt.

Hány darab PHL lehetséges összesen, ha a gépet n hosszú inputtal indítjuk?

$$\#PHL \leq |Q||T|^{S(n)}(n+1)S(n)^k \leq \text{konstans} \cdot c_2^{S(n)} =: t,$$

(az $(n+1)$ tényező az input fej lehetséges helyzeteinek a száma, az $S(n)^k$ tényező pedig a többi fej lehetséges helyzeteinek a száma)

Ha t lépés után leljük \checkmark de lehet, hogy t nem rekurzív \checkmark

N konstrukciója: megduplázzuk M -et $\rightarrow M_1$ és M_2

M_1 -et elindítjuk az x inputtal.

Minden egyes lépése után ideiglenesen megállítjuk

\rightarrow ekkor M_2 -t elindítjuk x inputtal a kezdő állapotból, és működtetjük legfeljebb addig a lépésig, ahol M_1 tart (\rightarrow ennek sorszámát l , amit $O(S(n))$ extra cellán tárolunk és léptetünk.)

Ha valamely $j < l$ -re az M_2 gép j -edik lépés utáni PHL-je megegyezik M_1 -ével \implies végtelen ciklus $\implies x \notin L \implies N$ megáll elutasítva x -et

Ha ilyen ismétlődés nem fordult elő, akkor meglépjük M_1 következő, $l + 1$ -edik lépését, stb.

ha M_1 megáll elfogadva (elutasítva) x -et $\implies N$ is megáll elfogadva (elutasítva) x -et.

\implies felismerjük a végtelen ciklusokat

mindig teljesül $l \leq t \implies$ a maximális futási idő legfeljebb

$$O(t^2) = O((c_2^{S(n)})^2) = O((c_2^2)^{c_1 S(n)}) \implies c = c_2^{2c_1} \checkmark$$

a tárfelhasználás közben nem nőtt lényegesen

Tétel. Ha $f \in FSPACE(s(n))$, akkor van olyan f -től függő c konstans, mellyel $f \in FTIME(c^{s(n)})$.

Tétel. $TIME(t(n)) = coTIME(t(n))$.

Bizonyítás: Megcseréljük M elfogadó és elutasító (azaz nem elfogadó) állapotait ✓

Tétel. $SPACE(s(n)) = coSPACE(s(n))$.

Bizonyítás: Alkalmazzuk a tár–idő-tétel szimulációját. Az adódó N TG szintén $O(s(n))$ tárkorlátos, és *minden inputra megáll*.

Most cseréljük fel az elfogadó és az elutasító állapotokat.

Definíció. $EXPTIME := \cup_{k \geq 1} TIME(2^{n^k})$.

Definíció. $PSPACE := \cup_{k \geq 1} SPACE(n^k)$.

Tétel. $P \subseteq \underline{\text{PSPACE}} \subseteq \underline{\text{EXPTIME}}$

Bizonyítás: Ha M egy $t(n)$ időkorlátos TG $\implies ct(n)$ tárkorlátos \iff
 $\implies \text{TIME}(n^k) \subseteq \underline{\text{SPACE}}(n^k) \implies P \subseteq \underline{\text{PSPACE}}$ ✓

Legyen $L \in \text{PSPACE} \implies L \in \text{SPACE}(n^k)$, valamely k -ra
 tár-idő-tétel \implies van olyan $c > 0$, hogy

$L \in \text{TIME}(c^{n^k}) \subseteq \text{TIME}(2^{\lceil c \rceil n^k}) \subseteq \text{TIME}(2^{n^{k+1}}) \subseteq \underline{\text{EXPTIME}}$. ✓

Tétel. $\text{TIME}(t(n)) \subset \mathcal{R}$, $\text{SPACE}(s(n)) \subset \mathcal{R}$ és $\text{EXPTIME} \subset \mathcal{R}$.

Bizonyítás: Csak azt látjuk be, hogy $\exists L$ rekurzív nyelv, hogy $L \notin \text{EXPTIME}$, a többi állítás hasonlóan kijön

$L = \{w \in I^*; \text{ az } M_w \text{ TG létezik, és legfeljebb } 2^{2^{|w|}} \text{ lépésben elutasítja } w\text{-t}\}$.

Ez rekurzív, mert mindig megálló univerzális TG felismeri.

Belátjuk, hogy $L \notin \text{TIME}(2^{2^{n-1}})$

Indirekt, tegyük fel, hogy L felismerhető egy $c2^{2^{n-1}}$ időkorlátos M TG-vel.

Legyen n_0 olyan nagy, hogy $c2^{2^{n-1}} < 2^{2^n}$ teljesüljön, ha $n > n_0$.

Legyen w egy n_0 -nál hosszabb szó, melyre M_w létezik, és ugyanúgy viselkedik mint M (ilyen van).

\implies ha $w \in L$, akkor M_w elfogadja w -t $c2^{2^{|w|}-1} < 2^{2^{|w|}}$ lépésben

$\implies w \notin L$

fordítva is \downarrow

Nemdeterminisztikus Turing-gépek

Olyan TG, ahol az átmenetfüggvény nem igazi függvény, több lehetőség van:

$$\delta(q, a) \subseteq Q \times T \times \{\text{jobb, bal, helyben}\}.$$

Gép futása, számítási út: Mint a TG, csak ha több lehetőség van, választ egyet, ha nincs értelmezve, akkor megáll.

Definíció. Az M NTG **elfogadja** az $x \in I^*$ inputot, ha az M -et x bemenettel a kiinduló helyzetből indítva van legalább egy elfogadó (egy elfogadó állapotban véget érő) számítási út.

Tétel. Az $x \in I^*$ input szó pontosan akkor nincs L_M -ben, ha az M gépet x inputtal indítva nincs elfogadó számítási út.

NTG számítási \implies gyökeres fa \implies csúcsok \leftrightarrow PHL

Időkorlátos NTG

Definíció. Egy M *nemdeterminisztikus Turing-gép* $t(n)$ *időkorlátos*, ha n hosszúságú inputokon M *minden számítási út mentén legfeljebb* $t(n)$ *lépést téve megáll.*

Senki nem tud egy $t(n)$ időkorlátos NTG-t $O(t(n))$ időben szimulálni.

Definíció. $NTIME(t(n)) :=$
 $\{ \text{az } O(t(n)) \text{ időkorlátos NTG-k által elfogadott nyelvek} \}.$

Definíció. $NP := \cup_{k \geq 1} NTIME(n^k).$

Tétel. $P \subseteq NP.$

Bizonyítás: A NTG egyben TG is ugyanolyan időkorláttal
 $\implies TIME(n^k) \subseteq NTIME(n^k) \implies \checkmark$

A legfontosabb megoldatlan probléma

P = ? NP

Tétel. $P \subseteq NP \cap \text{coNP}$.

Bizonyítás: $P \subseteq NP \implies \text{coP} \subseteq \text{coNP}$.

$P = \text{coP} \implies \checkmark$

Szintén megoldatlan problémák:

$$P \stackrel{?}{=} NP \cap \text{coNP}.$$

$$NP \stackrel{?}{=} \text{coNP}.$$

Nemdeterminisztikus felismerés

Hogyan tudjuk belátni, hogy $L \in \text{NP}$?

Legyen M kétszalagos **determinisztikus** TG, inputja két részből áll, egyik része $x \in I^*$ az első szalagon van, a másik része $y \in I^*$ a másikon \implies ez csak olvasható

\implies az M **súgásszalagja**

Az M által felismert L_1 nyelv \implies azon (x, y) szó párok halmaza $(x, y \in I^*)$, melyeket M elfogad

Definíció. Az M által **nemdeterminisztikusan** felismert L nyelv a következő:

$x \in L$ akkor, és csak akkor, ha van olyan y súgás, hogy $(x, y) \in L_1$.

Nem tudunk semmit arról, hogyan lehet jó súgást találni.

Tanú-tétel

Tétel. *[tanú-tétel] Egy $L \subseteq I^*$ nyelvre a következő két állítás egyenértékű:*

(a) $L \in \text{NP}$.

(b) *Van olyan $c > 0$ állandó, továbbá egy $L_1 \in \text{P}$ nyelv, mely olyan $(x, y) \in (I^*)^2$ párokból áll, hogy $|y| \leq |x|^c$ és $x \in I^*$ esetén $x \in L$ pontosan akkor, ha van $y \in I^*$ úgy, hogy $(x, y) \in L_1$.*

Bizonyítás: (a) \Rightarrow (b) :

$L \in \text{NP} \Rightarrow \exists n^{c_1}$ időkorlátos N NTG, mely felismeri L -et

Tegyük fel, hogy N -nek egy lépésnél legfeljebb d elágazási lehetősége van

Adunk egy M -et és egy megfelelő sűgást

$x \in L, |x| = n \Rightarrow y = y_1 y_2 \cdots y_m$ legyen az x elfogadását leíró számítási útja

$$\Rightarrow |y| \leq n^{c_1} \lceil \log_2(d+1) \rceil \leq n^c$$

Az M TG szimulálja N -et, úgy hogy mindig a kijelölt úton megy tovább
 N egy lépését konstans időben szimulálja.

N futási ideje éppen $c_2|y| \Rightarrow M$ futása az inputhoz képest lineáris

Ha viszont $x \notin L \Rightarrow (x, y) \notin L_1 = L_M$ tetszőleges $y \in I^*$ -ra ✓

$(b) \Rightarrow (a)$: Egy $x \in L$ inputhoz a feltétel szerint van legfeljebb n^{c_1} hosszúságú y , hogy $(x, y) \in L_1$.

Legyen N olyan mint M , de amikor M y -ből olvasna 0-t vagy 1-et $\Rightarrow N$ -ben δ -ra két lehetőség

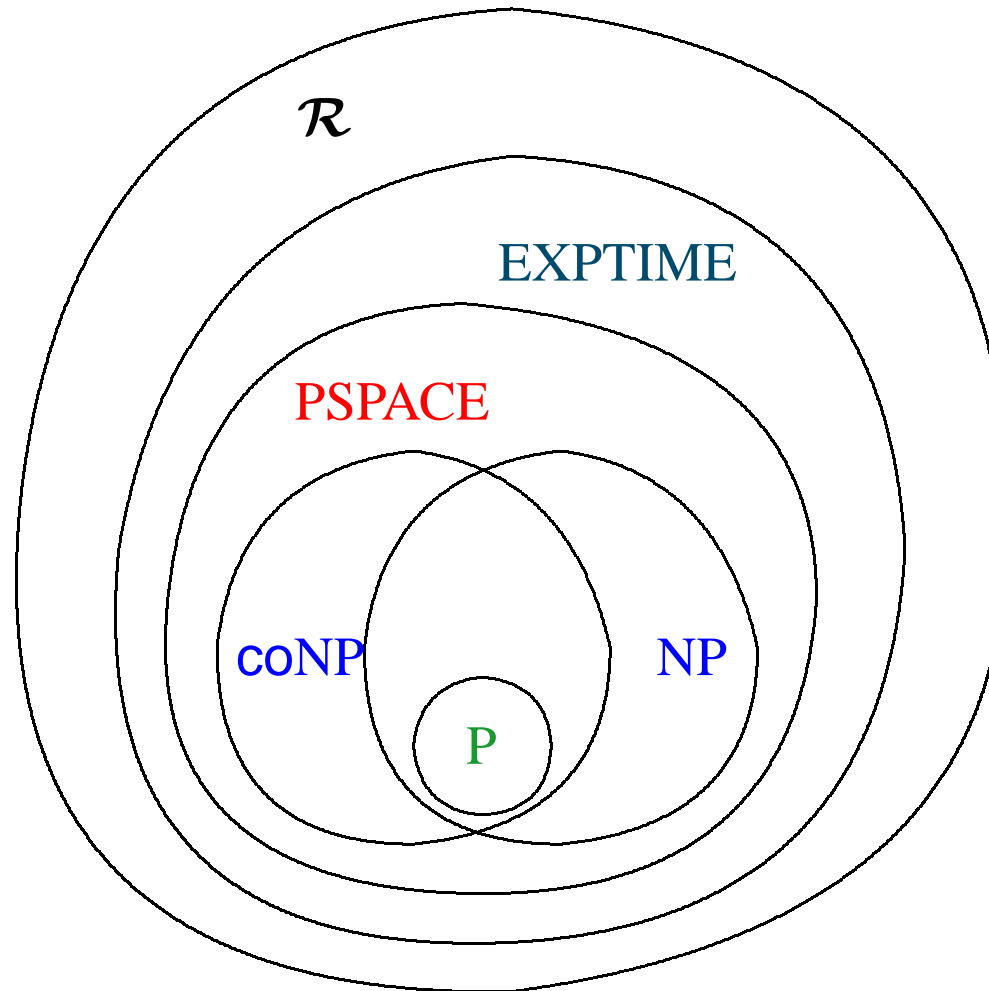
Az N NTG n^{c_2} időkorlátos ✓

Tétel. $NP \subseteq PSPACE$

Bizonyítás: Ha $L \in NP \Rightarrow \exists$ sűgás

Adott $x \in L$ -re végigpróbáljuk az összes n^c szóba jövő sűgást

Ez nagyon sokáig tart, de csak $\log_2 2^{n^c} = n^c$ tár kell hozzá



Sejtés: $P \neq PSPACE$

$NP \neq coNP \Rightarrow P \neq NP \Rightarrow PSPACE \neq P$