Algoritmuselmélet 15. előadás

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

2002 Április 23.

NP-beli nyelvek

A tanú tétel segítségével könnyű belátni, hogy egy nyelv NP-beli.

Csak azt kell belátni, hogy létezik tanú, megkeresni nem kell tudni.

A mi szerepünk a bíró szerepe, nem a nyomozóé.

3 színnel színezhető gráfok

$G \rightarrow$ pl. adjacencia mátrix sorai egymásután fűzve
$x \in$ 3-SZÍN $\Longrightarrow$ ha az x szónak megfelelő gráf 3 színnel színezhető.

Tétel. *3-SZÍN* $\in$ NP.

Bizonyítás: Alkalmas tanú G egy jó színezése
Ez leírható $2n$ bittel $\Longrightarrow$ (pl.legyen 01=piros, 10=sárga, 11=zöld)

G, színezés $\rightarrow$ bíró $\Longrightarrow$ jó színezés-e
Ez polinom időben megtehető TG-vel.
Ha G nem 3-színezhető, akkor nem lehet tanúja.

Hamilton-körrel rendelkező gráfok

$H \implies$ Azon gráfok szavai, amik tartalmaznak Hamilton-kört.

Tétel. *$H \in$ NP.*

Bizonyítás: A $G \in$ H állításnak rövid tanúja egy Hamilton-kör.
csúcsok sorrendje $\implies O(n \log n)$ bit
a bíró ellenőrzi, hogy van-e él a következő csúcsba G-ben.

Hasonlóan Hamilton-útra, irányított Hamilton-körre, -útra

Legyen NH a Hamilton-kört nem tartalmazó gráfok nyelve.

Tétel. *$NH \in$ coNP.*

Síkba rajzolható gráfok

Legyen L a síkba rajzolható gráfok nyelve

Tétel. $L \in \mathrm{NP}$

Bizonyítás: G tanúja egy síkbarajzolása.
Fáry-Wágner $\Longrightarrow$ van olyan is, ami egyenes szakaszokat használ. Sőt olyan is van, hogy a koordináták nem túl nagyok.
$\Longrightarrow$ Tanú a csúcsok koordinátái.
A bíró ellenőrzi, hogy az élek nem metszik egymást.

Tétel. $L \in \mathrm{coNP}$ *(* $\Longrightarrow L \in \mathrm{NP} \cap \mathrm{coNP}$*: jól karakterizált)*

Bizonyítás: Van tanú a $G \notin L$ állításra is.
Vagy nem gráf vagy Kuratowski $\Longrightarrow$ van benne vagy K_5-tel vagy $K_{3,3}$-mal topologikusan izomorf részgráf.
Tanú egy ilyen leírása, ezt a bíró könnyen ellenőrizheti.
Tétel. $L \in \mathrm{P}$

Sejtés: $H \notin \mathrm{coNP}$ és 3-SZÍN $\notin \mathrm{coNP}$

A prímszámok nyelve

Jelölje $\mathbf{\Pi}$ a (binárisan ábrázolt) prímszámok nyelvét.

Tétel. [V. R. Pratt, 1975]

$$\mathbf{\Pi} \in \mathrm{NP} \cap \mathrm{coNP}.$$

Bizonyítás: $\mathbf{\Pi} \in \mathrm{coNP}$: Ha egy szám nem prím, arra tanú egy osztója, pl. 6 nem prím, mert $\mathbf{2|6}$.

$\mathbf{\Pi} \in \mathrm{NP}$:
Lemma. *Legyen $p \geq 2$ egy egész szám. A p pontosan akkor prímszám, ha van olyan $1 \leq g < p$ egész, melyre teljesülnek az alábbiak:*

1. $g^{p-1} \equiv 1 \pmod{p}$,

2. $g^{\frac{p-1}{r}} \not\equiv 1 \pmod{p}$ *minden r prímszámra, melyre $r|p-1$.*

Gyors hatványozás: a^m alakú hatvány legfeljebb $2\log_2 m$ szorzással kiszámítható.
$m = e_0 + e_1 2^1 + e_2 2^2 + \cdots + e_k 2^k$, $k \leq \log_2 m$ és $e_j \in \{0,1\}$.
Ismételt négyzetre emelésekkel $\Longrightarrow a^{2^j}$ $\Longrightarrow$ ez k szorzás
szorozzuk össze az a^{2^j} hatványokat azokra a j értékekre, melyekre $e_j = 1$
$\Longrightarrow a^m = a^{e_0 + e_1 2^1 + e_2 2^2 + \cdots + e_k 2^k} = a^{e_0} a^{e_1 2^1} a^{e_2 2^2} \cdots a^{e_k 2^k}$
$\Longrightarrow k$ szorzás

a^m mérete $m + a$ méretében exponenciális $\Longrightarrow$ exponenciális alg.
$a^m \pmod n$ mérete legfeljebb $\log_2 n$ $\Longrightarrow$ ha mindig a maradékot vesszük
$\Longrightarrow$ polinomiális alg.

A p *prím állításra* tanú: g és $p-1$ egész $r_1, \ldots, r_k$ prímosztói
a bíró gyors hatványozással ellenőrizheti, hogy a Lemma feltételei teljesülnek.
Azt is tanúsítani kell, hogy $r_1, \ldots, r_k$ éppen a $p-1$ prímosztói (más nincs)
$\Longrightarrow$ prímtényezős felbontás $\surd$
és azt is, hogy $r_1, \ldots, r_k$ prímek $\Longrightarrow$ rekurzívan $\surd$
Belátható, hogy a tanú össz mérete $O(n^2)$.

Tétel. [M. Agrawal, N. Kayal, N. Saxena, 2002] $\Pi \in \mathrm{P}$

Felismerés és keresés

Prím-e $\leftrightarrow$ legkisebb prím osztója

$$F = \left\{ (a,c) \;\middle|\; \begin{array}{l} 1 < c \leq a \text{ egészek és van olyan } 1 < b \leq c \text{ egész,} \\ \text{melyre } b \text{ osztója } a\text{-nak} \end{array} \right\}.$$

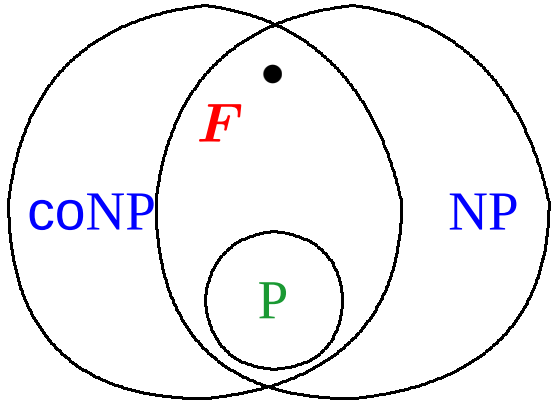
Tétel. $F \in \mathrm{NP} \cap \mathrm{coNP}$.

Bizonyítás: $(a,c) \in F \implies$ tanú egy jó b érték
$(a,c) \notin F \implies$ tanú $\rightarrow$ az $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ és a p_i számok prím-tulajdonságának tanúi

Legjobb ismert algoritmus a prím-felbontásra: D. Shanks $\implies$ n bites inputon $c2^{n/4}$.

Tétel. *Ha $F \in \mathrm{P}$ igaz lenne, akkor $\{$prímtényezős felbontás$\} \in \mathrm{FP}$ is igaz lenne.*

Bizonyítás: Legyen E egy gyors alg. F felismerésére
$(a, a-1) \in F$?
ha nem $\longrightarrow$ a prím $\surd$
ha igen $\Longrightarrow$ bináris kereséssel megkeressük a legkisebb olyan c-t amire $(a, c) \in F \Longrightarrow \leq \log_2 a$ hívás
Utána a/c-re folytatjuk . . .
$\Longrightarrow$ egy prím-osztó megtalálása: $O((\log a)^d)$
prím-osztók száma $\leq \log a$ $\Longrightarrow$ összköltség $O\left((\log a)^{d+1}\right)$



Karp-redukció

Mikor nem lényegesen nehezebb egy L_1 probléma egy L_2 problémánál?
$\Longrightarrow$ Ha L_2 felhasználásával meg lehet oldani L_1-et is.
$\Longrightarrow$ L_1 visszavezethető a L_2 problémára.

Definíció. *Az $f : I^* \to I^*$ leképezés az $L_1 \subseteq I^*$ nyelv* Karp-redukciója *az $L_2 \subseteq I^*$ nyelvre, ha*

1. *Tetszőleges $x \in I^*$ szóra $x \in L_1$ pontosan akkor teljesül, ha $f(x) \in L_2$;*

2. *$f \in FP$, azaz f polinom időben számítható.*

Jelölés: $L_1 \prec L_2$ ha L_1-nek van Karp-redukciója L_2-re.

Ha tehát van algoritmusunk L_2 eldöntésére $\Longrightarrow$ $x \in L_1$-re kiszámítjuk $f(x)$-et eldöntjük $f(x) \in L_2$? $\Longrightarrow$ tudjuk, hogy $x \in L_1$ igaz-e $\surd$

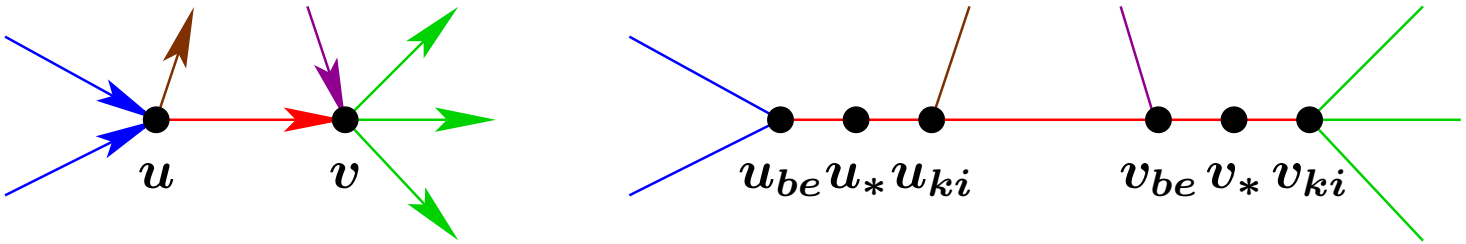
Ha tudnánk, hogy L nehéz és tudjuk, hogy $L \prec L'$ $\Longrightarrow$ L' is nehéz lenne
Ha L' könnyű lenne, és L nem lényegesen nehezebb nála, akkor L is könnyű.

Irányított Hamilton-kör probléma

Tétel. *IH* $\prec$ *H.*

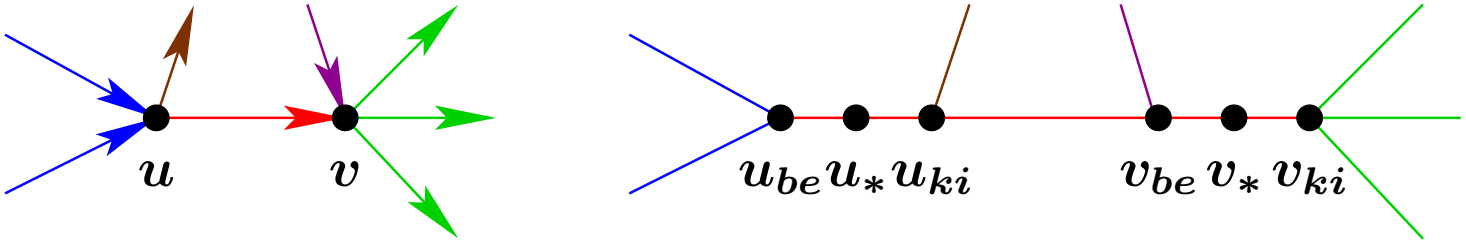
Bizonyítás: $G = (V, E)$ egy irányított gráf $\longrightarrow G' = (V', E')$ irányítatlan gráf hogy G' gyorsan megépíthető és
G-ben $\exists$ irányított Hamilton-kör $\leftrightarrow$ G'-ben $\exists$ irányítatlan Hamilton-kör.

$$\begin{aligned} V' &= \{v_{be}, v_*, v_{ki} \mid v \in V\}, \\ E' &= \{(v_{be}, v_*), (v_*, v_{ki}) \mid v \in V\} \cup \{(u_{ki}, v_{be}) \mid u \longrightarrow v \in E\}. \end{aligned}$$



$v(G) = n, e(G) = e \implies v(G') = 3n, e(G') = 2n + e \implies (n + e)^c$ lépésben megkapható.

G-beli F irányított Hamilton-körének $\implies G'$ egy F' Hamilton-köre



Az F egy $u \to v$ éle $\Longrightarrow$ az F'-ben az $u_* - u_{ki} - v_{be} - v_*$ út
$\Longrightarrow \boldsymbol{G \in IH} \Longrightarrow \boldsymbol{G' \in H}$

Ha G'-ben van egy $F' \subseteq E'$ Hamilton-kör $\Longrightarrow$ egy u_*-ból indulva egy u_{ki} felé lépjünk először
$\Longrightarrow$ csak $u_* - u_{ki} - v_{be} - v_*$ alakú lehet utána $\Longrightarrow$ stb. $\Longrightarrow$ Ha $G' \in H$ akkor $G \in IH$.

A Karp-redukció felhasználása

Tétel.

1. Ha $L_1 \prec L_2$ *és* $L_2 \in \mathrm{P}$, *akkor* $L_1 \in \mathrm{P}$.
2. Ha $L_1 \prec L_2$ *és* $L_2 \in \mathrm{NP}$ *akkor* $L_1 \in \mathrm{NP}$.
3. Ha $L_1 \prec L_2$, *akkor* $\overline{L}_1 \prec \overline{L}_2$, *ahol* $\overline{L}_i = I^* \setminus L_i$.
4. Ha $L_1 \prec L_2$ *és* $L_2 \in \mathrm{coNP}$, *akkor* $L_1 \in \mathrm{coNP}$.
5. Ha $L_1 \prec L_2$ *és* $L_2 \in \mathrm{NP} \cap \mathrm{coNP}$, *akkor* $L_1 \in \mathrm{NP} \cap \mathrm{coNP}$.
6. Ha $L_1 \prec L_2$ *és* $L_2 \prec L_3$, *akkor* $L_1 \prec L_3$.

Bizonyítás:

Legyen $f : I^* \to I^*$ az L_1 Karp-redukciója L_2-re, $f \in FTIME(n^k)$.
$x \in I^*$ egy input szót, melyre szeretnénk eldönteni, hogy $x \in L_1$ teljesül-e, n az x hossza.

1. Kiszámítjuk $f(x)$-et $\Longrightarrow$ időigénye $\leq c_1 n^k$ $\Longrightarrow |f(x)| \leq c_1 n^k$
L_2 felismerő algoritmusával eldöntjük, hogy $f(x) \in L_2$ igaz-e
$\Longrightarrow$ időigénye $\leq c_2 (c_1 n^k)^l$
$x \in L_1 \leftrightarrow f(x) \in L_2$ $\Longrightarrow$ összidő $O(n^{kl})$ $\surd$

2.: Ha $L_1 \prec L_2$ és $L_2 \in \mathrm{NP}$ akkor $L_1 \in \mathrm{NP}$: Az $f(x) \in L_2$ tény egy y tanúja jó $x \in L_1$ tanújának is, és az L_2-höz tartozó bíró egy kis módosítással jó lesz az L_1 bírójának is
$|y| \leq |f(x)|^c \implies |y| \leq c_1^c |x|^{kc}$
Az L_1 bírója az $(x, y) \to f(x) \implies (f(x), y) \to L_2$ bírájának
L_1 bírója pontosan akkor fogadja el az (x, y) párt $\leftrightarrow$ L_2 bírója elfogadja az $(f(x), y)$ párt

3.: Ha $L_1 \prec L_2$, akkor $\overline{L_1} \prec \overline{L_2}$: Mint 1. hiszen $x \in I^*$ szóra $x \notin L_1 \leftrightarrow f(x) \notin L_2$.

4.: Ha $L_1 \prec L_2$ és $L_2 \in \mathrm{coNP}$, akkor $L_1 \in \mathrm{coNP}$: $\Longleftarrow$ 2.,3.

5.: Ha $L_1 \prec L_2$ és $L_2 \in \mathrm{NP} \cap \mathrm{coNP}$, akkor $L_1 \in \mathrm{NP} \cap \mathrm{coNP}$.: $\Longleftarrow$ 2.,4.

6.: Ha $L_1 \prec L_2$ és $L_2 \prec L_3$, akkor $L_1 \prec L_3$: Legyen f az $L_1 \prec L_2$ függvénye, ami $O(x^k)$ időben számolható
és g az $L_2 \prec L_3$ függvénye, ami $O(x^l)$ időben számolható
Az $L_1 \prec L_3$ függvénye $g(f(x))$ lesz, ami $O((x^k)^l) = O(x^{kl})$ időben számolható

NP-teljes nyelvek

Definíció. *Az $L \subseteq I^*$ nyelv NP-teljes, ha*

1. $L \in \mathrm{NP}$,

2. tetszőleges (azaz minden) $L' \in \mathrm{NP}$ nyelv esetén létezik $L' \prec L$ Karp-redukció.

Egy NP-teljes nyelv tehát legalább olyan nehéz, mint bármely más NP-beli nyelv.

Ha egy ilyen nyelvről kiderülne, hogy P-beli (coNP-beli), akkor ugyanez igaz lenne minden NP-beli nyelvre.

Van-e NP-teljes nyelv?

Cook–Levin-tétel

Boole-formula:
pl. $(x_1 \vee \overline{x_2} \vee x_5) \wedge (\overline{x}_3 \vee x_2 \vee x_6 \vee x_1) \wedge \overline{(x_5 \vee x_6)}$

Definíció. *SAT nyelv: a kielégíthető Boole-formulák nyelve.*
Tétel. *[S. A. Cook, L. Levin, 1971]*
A SAT nyelv NP*-teljes.*

Bizonyítás: SAT $\in NP$, mert egy kielégítés (értékadás a változóknak) megfelelő tanú ✓

Be kell látni, hogy $\forall L \in \mathrm{NP}$ nyelvre létezik egy $L \prec$ SAT Karp-redukció
$\Longrightarrow (x \in L?)$ kérdés tetszőleges $x \in I^*$ inputjához meg kell adnunk egy ϕ Boole-formulát, mely pontosan akkor kielégíthető, ha $x \in L$.
$\Longrightarrow$ tanú-tétel miatt elég leírni Boole-formulával az (x, y)-t felismerő TG-t

$$\mathbf{0}x[i,j] = \begin{cases} \mathbf{1} & \text{ha az } i\text{-edik lépés után a } j\text{-edik cella tartalma 0} \\ \mathbf{0} & \text{különben} \end{cases}$$

$$\mathbf{1}x[i,j] = \begin{cases} \mathbf{1} & \text{ha az } i\text{-edik lépés után a } j\text{-edik cella tartalma 1} \\ \mathbf{0} & \text{különben} \end{cases}$$

$$\text{ü}x[i,j] = \begin{cases} \mathbf{1} & \text{ha az } i\text{-edik lépés után a } j\text{-edik cella tartalma ü} \\ \mathbf{0} & \text{különben} \end{cases}$$

$$f[i,j] = \begin{cases} \mathbf{1} & \text{ha az } i\text{-edik lépés után a fej } j\text{-edik cellán áll} \\ \mathbf{0} & \text{különben} \end{cases}$$

$$q[i,s] = \begin{cases} \mathbf{1} & \text{ha az } i\text{-edik lépés után } M \text{ belső állapota } q_s \\ \mathbf{0} & \text{különben.} \end{cases}$$

Le kell írni $\Longrightarrow$ a szalag egy mezőjén minden időpontban éppen egy szalagjel van; a fej minden időpontban a szalag egyetlen celláján van; a gép minden időpontban egyetlen állapotban van.
pl. az első: ($0 \leq i \leq n^c$, $1 \leq j \leq n^c$) párra

$$(0x[i,j] \vee 1x[i,j] \vee \text{ü}x[i,j]) \wedge$$

$$\wedge(\overline{0x[i,j]} \vee \overline{1x[i,j]}) \wedge (\overline{0x[i,j]} \vee \overline{\text{ü}x[i,j]}) \wedge (\overline{1x[i,j]} \vee \overline{\text{ü}x[i,j]}).$$

Összesen $(n^c+1)n^c$ ilyen formula

Átmenet függvény leírása: pl. $\delta(q_s,1) = (q_k,0,bal) \Longrightarrow$

$$\Big((q[i,s] \wedge 1x[i,l] \wedge f[i,l]) \longrightarrow (q[i+1,k] \wedge 0x[i+1,l] \wedge f[i+1,l-1])\Big)$$

$O(n^{2c})$ ilyen formula

Ahol nincs fej, nincs változás:

$$\overline{f[i,l]} \longrightarrow (0x[i,l] \leftrightarrow 0x[i+1,l])$$

$O(n^{2c})$ ilyen formula (1-re és ü-re is)

Kezdő helyzet:

$$q[0,0] \wedge f[0,1]$$

Input leírása:

$$0x[0,1] \wedge 1x[0,2] \wedge 0x[0,3] \ldots$$

Elfogadó állapot:

$$1x[n^c,1]$$

Minden ilyen $i = 0,1,2,\ldots,n^c$-re ÉS-sel
Szabadsági fok: a súgás helyén nincs megkötve semmi

Ez a Boole formula akkor és csak akkor kielégíthető, ha van megfelelő súgás x-hez. $\surd$

További NP-teljes feladatok

Tétel. *Ha az* L_1 *nyelv* NP*-teljes,* $L_2 \in \text{NP}$ *és* $L_1 \prec L_2$*, akkor* L_2 *is* NP*-teljes.*

Bizonyítás: Láttuk, hogy a Karp-redukció tranzitív
Ha $L_1 \prec L_2$ és $L' \prec L_1 \; \forall L' \in$ NP-teljes
$\Longrightarrow L' \prec L_2 \; \forall L' \in$ NP-teljes $\surd$

Nem kell már *minden* NP-beli nyelvet az L_2-re redukálni; elég ezt megtenni *egyetlen* NP-teljes L_1 nyelvvel.

Definíció. *Ha az* L_2 *nyelvről csak azt tudjuk, hogy van olyan* NP*-teljes* L_1 *nyelv, melyre* $L_1 \prec L_2$*, akkor* L_2*-t* NP-nehéz *nyelvnek nevezzük. Az előző állítás szerint* L_2 *pontosan akkor* NP*-teljes, ha* NP*-beli és ugyanakkor* NP*-nehéz is.*