Matematikai logika

2010/2011 ősz

11. előadás

Definíció: *nemdeterminisztikus Turing gép*

$T = \langle \Gamma, Q, \delta \rangle$ egy nemdeterminisztikus Turing gép, ha

- Γ: a szalagábécé, egy véges halmaz;
  $* \in \Gamma$, ahol $*$ az üres karakter a szalagon
- Q: az állapotok véges halmaza
  $START, STOP \in Q$ a kezdő és az elfogadó állapot.
- δ: az állapotátmenet-reláció:
  $\delta \subseteq (\Gamma \times Q) \times (\Gamma \times Q \times \{-1, 0, 1\})$ ahol $\{-1, 0, 1\}$: hátra lép, helyben marad, előre lép

Emlékeztető: *L nyelv NP-beliségе*

Egy $L \subseteq \Gamma^*$ nyelv NP-beli, ha van olyan nemdeterminisztikus T-gép és $c_1, c_2 \in \mathbb{R}$ ($\in \mathbb{N}$ is lehetne) úgy, hogy tetszőleges $w \in \Gamma^*$-ra: $w \in L \Leftrightarrow$ T elfogadja w-t legfeljebb $c_1|w|^{c_2}$ lépésben.

Tétel:

Legyen sat = „a kielégíthető konjunktív normál formák halmaza”.
Ekkor sat NP-teljes.

Bizonyítás:

1) sat NP-beli ($sat \in NP$), erre tanú egy interpretáció, ami igazzá teszi a kérdéses formulát.

2) Megmutatjuk, hogy sat NP-nehéz, tehát bármely $L \in NP$ nyelv polinom időben redukálható sat-ra.

$L \in NP \Rightarrow$ van $T = \langle \Gamma, Q, \delta \rangle$ nemdeterminisztikus Turing gép és van c_1, c_2 szám, hogy a T Turing-gép $\leq c_1|w|^{c_2}$ lépésben helyes választ ad a $w \in L$ kérdésre, ha tényleg $w \in L$. Rögzítsük $w \in \Gamma^*$-t, és vezessük be az ítéletváltozók következő rendszerét:

Legyen $N = \lceil c_1|w|^{c_2} \rceil$

Legyen $X[n, p]$	$0 \leq n \leq N, \quad P \in Q$’
Legyen $Y[n, k]$	$0 \leq n \leq N, \quad -N \leq k \leq N$’
Legyen $Z[n, p, k]$	$0 \leq n \leq N, \quad -N \leq p \leq N, \quad k \in \Gamma.$

A szándékolt jelentés:

$X[n, p]$:	az n. lépés után T a p állapotban van,
$Y[n, k]$:	az n. lépés után a gép feje a k. pozíción áll,
$Z[n, p, k]$:	az n. lépés után a szalag p. pozícióján „k” szerepel.

Axiomatizáljuk T működését: megadunk egy φ formulát úgy, hogy φ hossza polinom $|w|$-ben és φ pont akkor elégíthető ki, ha T elfogadja w-t. φ-t az alábbi lépésekkel adjuk meg:

(a) T mindig van valamilyen állapotban:

$$\left(\bigvee_{p \in Q} X[1, p] \right) \wedge \left(\bigvee_{p \in Q} X[2, p] \right) \wedge \cdots \wedge \left(\bigvee_{p \in Q} X[N, p] \right)$$

(b) T csak egy állapotban van:
$\{\neg X[n,p] \vee \neg X[n,q] : p \neq q \in Q, 0 \leq n \leq N\}$.

(c) a fej minden lépésben pontosan egy helyen van:

- van valahol
- nincs két helyen

(a) és (b) mintájára elképzelhető

(d) minden mezőn pont egy jel áll:

- áll valamin
- nem áll kettőn

(a) és (b) mintájára elképzelhető

(e) a 0. lépésben a START mezőn áll:
$X[0, START]$
az utolsó lépés után a STOP mezőn áll:
$X[N, STOP]$

(f) kezdetben $w = w_1 w_2 \ldots w_k$ van a szalagon:
$\{Z[0, i-1, w_i],\ ha\ 1 \leq i \leq k\} \cup \{Z[0, i-1, *],\ ha\ i \leq 0\ vagy\ i > k\}$

(g) a gép a δ átmenetreláció szerint működik:
ha $q, q' \in Q,\ v, v' \in \Gamma,\ \varepsilon \in \{-1, 0, 1\},\ -N \leq p \leq N,\ (q, v, q', v', \varepsilon) \notin \delta$ akkor:
$\neg X[n,q] \vee \neg Y[n,p] \vee \neg Z[n,p,v] \vee \neg X[n+1,q'] \vee \neg Y[n+1,p+k] \vee \neg Z[n+1,p,v']$
(tehát a gép nem tud a (q,v) állapotból a (q',v')-be lépni)

(h) ahol nem áll fej, ott nem változik a szalag tartalma:
$(Y[n,p] \vee Z[n,p,v] \vee \neg Z[n+1,p,v]) \wedge (Y[n,p] \vee \neg Z[n,p,v] \vee Z[n+1,p,v])\ \forall n,p,v$

Legyen $\varphi = (a) \wedge (b) \wedge \ldots \wedge (h)$.
T elfogadja w-t pont akkor, ha φ kielégíthető.
■

Definíció: *n-sat*
Olyan kielégíthető konjunktív normál formák, melyek elemi diszjunkcióiban legfeljebb $n (\in \mathbb{N})$ változó fordul elő.

Példa: $(X_1 \vee \neg X_2) \wedge (X_1 \vee X_3 \vee X_{17}) \wedge (X_{15} \vee \neg X_1) \in$ *3-sat*

Tétel:
3-sat NP teljes.

Bizonyítás:
1) *3-sat* NP-beli ($\in NP$), hiszen a *3-sat*-nál általánosabb *sat* is NP-beli.
2) Elég bebizonyítani, hogy az NP-teljes *sat* redukálható *3-sat*-ra. A konstrukció: legyen φ tetszőleges konjunktív normál forma:
$\varphi = (X_1 \vee \ldots \vee X_k) \wedge (\ldots \vee \ldots) \wedge (\ldots \vee \ldots)$
A $(X_1 \vee \ldots \vee X_k)$ tagon bemutatjuk, az átalakítást (a többi tagon ugyanígy történik).

Ötlet:

$$\begin{array}{lcl} Y_1 = X_1 & \longleftrightarrow & Y_1 \Leftrightarrow X_1 \\ Y_2 = Y_1 \vee X_2 & \longleftrightarrow & Y_2 \Leftrightarrow Y_1 \vee X_2 \\ Y_3 = Y_2 \vee X_3 & \longleftrightarrow & Y_3 \Leftrightarrow Y_2 \vee X_3 \\ & \vdots & \end{array}$$

Megvalósítás: Cseréljük ki φ diszjunkciós komponenseit a következő módon (csak az első komponensre mutatjuk):

$$\begin{array}{lcll} Y_1 \Leftrightarrow X_1 & \longleftrightarrow & (\neg Y_1 \vee X_1) \wedge (\neg X_1 \vee Y_1) & (1) \\ Y_2 \Leftrightarrow Y_1 \vee X_2 & \longleftrightarrow & (\neg Y_2 \vee Y_1 \vee X_2) \wedge (Y_2 \vee \neg Y_1) \wedge (Y_2 \vee \neg X_2) & (2) \\ & \vdots & & \end{array}$$

Legyen $\varphi' = (1) \wedge (2) \wedge \ldots$.

Ekkor $\varphi = \varphi'$ egyszerre elégíthető ki.
φ' polinomiális időben (sőt, lineáris időben) kiszámítható φ-ből.
■

Megjegyzés: *2-sat* P-beli; bizonyítás legközelebb.