Bevezetés a számításelméletbe

10. előadás

BONYOLULTSÁGELMÉLET

A továbbiakban eldönthető problémákkal foglalkozunk, ilyenkor a kérdés az, hogy milyen idő illetve tár tekintetében milyen hatékonyan dönthető el az adott probléma.

A bonyolultságelmélet (angolul: complexity theory) az egyes idő- és tárbonyolultsági osztályok egymáshoz való viszonyával foglalkozik.

Időbonyolultsági osztályok, $P \stackrel{?}{=} NP$

Definíció

- $\mathrm{TIME}(f(n)) = \{L \mid L$ eldönthető $O(f(n))$ időkorlátos determinisztikus TG-pel$\}$
- $\mathrm{NTIME}(f(n)) = \{L \mid L$ eldönthető $O(f(n))$ időkorlátos NTG-pel$\}$
- $\mathrm{P}=\bigcup_{k\geq 1}\mathrm{TIME}(n^k)$.
- $\mathrm{NP}=\bigcup_{k\geq 1}\mathrm{NTIME}(n^k)$.

Észrevétel: $\mathrm{P} \subseteq \mathrm{NP}$, mivel minden determinisztikus TG tekinthető nemdeterminisztikusnak.

Sejtés: $\mathrm{P} \neq \mathrm{NP}$ (sejtjük, hogy igaz, de bizonyítani nem tudjuk).

A Clay Matematikai Intézet 2000-ben 7 probléma megoldására egyenként 1M$-t tűzött ki (Milleniumi problémák), ezek egyike a $\mathrm{P} \stackrel{?}{=} \mathrm{NP}$ probléma.

NP

P-re úgy gondolunk, hogy ez tartalmazza a gyakorlatban is hatékonyan megoldható problémákat. (Nem teljesen igaz.)

Milyen problémákat tartalmaz NP?

Egy L NP-beli problémához definíció szerint létezik őt polinom időben eldöntő NTG ami gyakran a következőképpen működik: a probléma minden I bemenetére polinom időben „megsejti” (azaz nemdeterminisztikusan generálja) I egy lehetséges m megoldását és polinom időben leellenőrzi (már determinisztikusan), hogy m alapján $I \in L$ teljesül-e. A NTG definíciója szerint elég egyetlen ilyen megoldást, „tanút” megsejteni.

Precíz tétellé is tehető, miszerint akkor és csak akkor NP-beli egy eldöntési probléma, ha minden igen-inputhoz megadható polinom méretű és polinom időben ellenőrizhető tanú (azaz, ami igazolja, hogy ő valóban igen-input).

A következőkben a P és NP bonyolultsági osztályok közötti kapcsolatot vizsgáljuk.

Polinom idejű visszavezetés

Definíció

Az $f : \Sigma^* \to \Delta^*$ szófüggvény **polinom időben kiszámítható**, ha van olyan polinom időkorlátos Turing gép, amelyik kiszámítja.

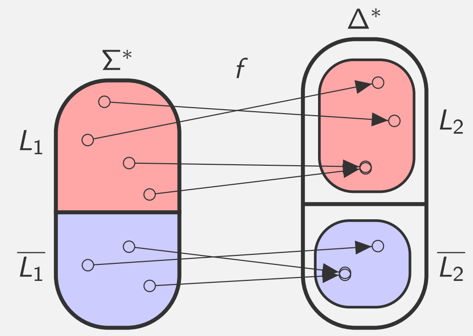
Definíció

$L_1 \subseteq \Sigma^*$ **polinom időben visszavezethető** $L_2 \subseteq \Delta^*$-ra, ha van olyan $f : \Sigma^* \to \Delta^*$ polinom időben kiszámítható szófüggvény, hogy $w \in L_1 \Leftrightarrow f(w) \in L_2$. Jelölés: $L_1 \leq_p L_2$.

Megjegyzés: A polinom idejű visszavezetést Richard Karpról elnevezve Karp-visszavezetésnek vagy Karp-redukciónak is nevezik. Angolul: polynomial-time many-one reduction vagy Karp reduction.

Polinom idejű visszavezetés

$L_1 \leq_p L_2$



f **polinom időben** kiszámítható, az egész Σ^*-on értelmezett, $f(L_1) \subseteq L_2$ valamint $f(\overline{L_1}) \subseteq \overline{L_2}$.

f nem kell hogy injektív legyen és az se, hogy szürjektív.

Tétel

- Ha $L_1 \leq_p L_2$ és $L_2 \in \mathrm{P}$, akkor $L_1 \in \mathrm{P}$.
- Ha $L_1 \leq_p L_2$ és $L_2 \in \mathrm{NP}$, akkor $L_1 \in \mathrm{NP}$.

Polinom idejű visszavezetés

Bizonyítás:

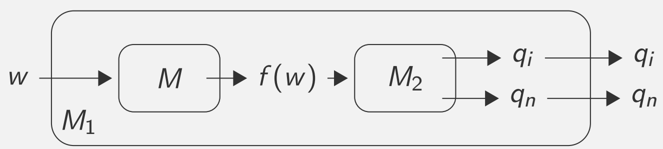
Az elsőt bizonyítjuk, a második analóg.

Legyen $L_2 \in$ P és tegyük fel, hogy $L_1 \leq_p L_2$.

Legyen M_2 az L_2-t eldöntő, míg M a visszavezetést kiszámító TG.

Feltehetjük, hogy M $p(n)$ és M_2 $p_2(n)$ polinom idejű TG-ek.

Konstruáljuk meg M_1-et:



- M_1 eldönti az L_1 nyelvet
- ha w n hosszú, akkor $f(w)$ legfeljebb $n + p(n)$ hosszú lehet (M minden lépése legfeljebb 1-gyel növelheti a hosszt.)
- M_1 tehát $p_2(n + p(n))$ időkorlátos, ami szintén polinom

$\mathcal{C}$-teljesség

Intuitíve, ha egy problémára visszavezetünk egy másikat, az azt jelenti, hogy az a probléma legalább olyan nehéz, mint amit visszavezettünk rá. Azaz ebben az értelemben a legnehezebb problémák azok, melyekre minden probléma visszavezethető.

Definíció

Legyen $\mathcal{C}$ egy bonyolultsági osztály. Egy L nyelv **$\mathcal{C}$-nehéz** (a polinom idejű visszavezetésre nézve), ha minden $L' \in \mathcal{C}$ esetén $L' \leq_p L$.

Definíció

Legyen $\mathcal{C}$ egy bonyolultsági osztály. Egy L nyelv **$\mathcal{C}$-teljes**, ha $L \in \mathcal{C}$ és L $\mathcal{C}$-nehéz.

Ilyen bonyolultsági osztályok pédául, P, NP, EXP (exponenciális időben eldönthető problémák osztálya), vagy a későbbiekben tanult tárbonyolultsági osztályok.

NP-teljesség

Ha speciálisan $\mathcal{C}$=NP:

NP-teljes nyelv

Egy L nyelv **NP-teljes** (a polinom idejű visszavezetésre nézve), ha

- $L \in$ NP
- L NP-nehéz, azaz minden $L' \in$ NP esetén $L' \leq_p L$.

Megjegyzés: Néha úgy fogalmazunk, hogy az L (eldöntési) probléma NP-teljes...

Tétel

Legyen L egy NP-teljes probléma. Ha $L \in$ P, akkor P = NP.

Bizonyítás: Elég megmutatni, hogy NP $\subseteq$ P.
Legyen $L' \in$NP egy tetszőleges probléma.
Ekkor $L' \leq_p L$, hiszen L NP-teljes.
Mivel $L \in$P, ezért az előző tétel alapján $L' \in$P.
Ez minden $L' \in$NP-re elmondható, ezért NP $\subseteq$ P.

Egy NP-teljes nyelv

Ha $L \leq_p L'$, akkor intuitíve L' legalább olyan nehéz, mint L. Így az NP-teljes problémák (ha vannak) az NP-beli problémák legnehezebbjei.

Az előző tétel szerint tehát, ha valaki talál egy NP-teljes problémára polinom idejű determinisztikus algoritmust, azzal bizonyítja, hogy P=NP.

Ezért nyilván egyetlen NP-teljes problémára sem ismeretes jelenleg polinomiális idejű determinisztikus algoritmus és nem túl valószínű, hogy valaha is fogunk ilyet találni. Így a gyakorlatban az NP-teljes problémákra úgy is tekinthetünk, mint bár eldönthető, de hatékonyan nem eldönthető problémákra.

Definíció

$\mathrm{SAT} := \{\langle\varphi\rangle \mid \varphi$ kielégíthető nulladrendű KNF$\}$

Cook-Levin tétel

SAT NP-teljes.

A Cook-Levin tétel bizonyítása

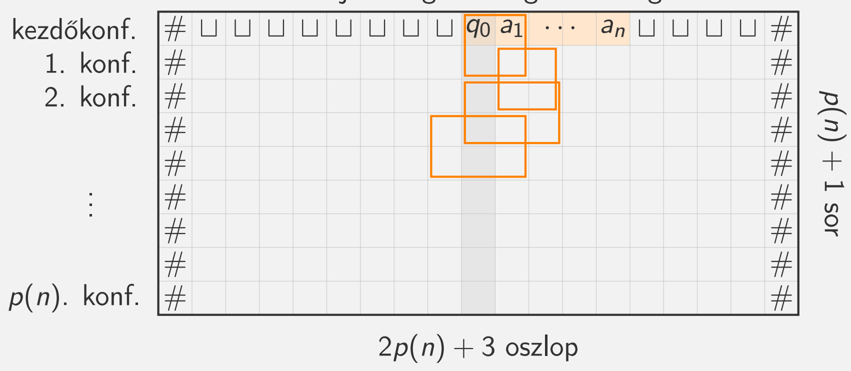
Bizonyítás:

- SAT$\in$ NP: Adott egy φ input. Egy NTG egy számítási ágán polinom időben előállít egy I interpretációt. Majd szintén polinom időben ellenőrzi, hogy ez kielégíti-e φ-t.
- SAT NP-nehéz: ehhez kell, $L \leq_p$ SAT, minden $L \in$ NP-re.

  • Legyen $M = \langle Q, \Sigma, \Gamma, \delta, q_0, q_i, q_n\rangle$ egy L-et eldöntő $p(n)$ polinom időkorlátos NTG. (Feltehető, hogy $p(n) \geq n$.)
  • Legyen továbbá $w = a_1 \cdots a_n \in \Sigma^*$ egy szó.
  • M segítségével megadunk egy polinom időben előállítható φ_w nulladrendű KNF formulát, melyre $w \in L \Leftrightarrow \langle\varphi_w\rangle \in$ SAT.
  • M egy számítása w-n leírható egy T táblázattal, melynek
  – első sora $\# \sqcup^{p(n)} C_0 \sqcup^{p(n)-n} \#$, ahol $C_0 = q_0 w$ M kezdőkonfigurációja w-n
  – T egymást követő két sora M egymást követő két konfigurációja (elegendő $\sqcup$-el kiegészítve, elején és a végén egy $\#$-el). Minden sor $2p(n)+3$ hosszú.

A Cook-Levin tétel bizonyítása

– $p(n)+1$ sor van. Ha hamarabb jut elfogadó konfigurációba, akkor onnantól kezve ismételjük meg az elfogadó konfigurációt.



– a konfigurációátmenet definíciója miatt bármely két sor közötti különbség belefér egy 2x3-as "ablakba"
– T magassága akkora, hogy minden, $\leq p(n)$ lépéses átmenetet tartalmazhasson. A $\sqcup$-ek számát ($\Rightarrow$ T szélességét) pedig úgy, hogy az ablakok biztosan "ne eshessenek le" egyik oldalon se.

A Cook-Levin tétel bizonyítása

– φ_w ítéletváltozói $x_{i,j,s}$ alakúak, melynek jelentése: T i-ik sorának j-ik cellájában az s szimbólum van, ahol $s \in \Delta = Q \cup \Gamma \cup \{\#\}$.
– φ_w a w bemenetre M minden lehetséges legfeljebb $p(n)$ lépésű működését leírja. Felépítése: $\varphi_w = \varphi_0 \wedge \varphi_{\text{start}} \wedge \varphi_{\text{move}} \wedge \varphi_{\text{accept}}$.
– φ_0 akkor és csak akkor legyen igaz, ha minden cellában pontosan 1 betű van:

$$\varphi_0 := \bigwedge_{\substack{1 \leq i \leq p(n)+1 \\ 1 \leq j \leq 2p(n)+3}} \left(\left(\bigvee_{s \in \Delta} x_{i,j,s} \right) \wedge \bigwedge_{s,t \in \Delta, s \neq t} (\neg x_{i,j,s} \vee \neg x_{i,j,t}) \right)$$

– φ_{start} akkor és csak akkor legyen igaz, ha T első sora a $\sqcup$-ekkel és $\#$-ekkel a fent említett módon adott hosszúságúra kiegészített kezdőkonfiguráció.

$$\varphi_{\text{start}} := x_{1,1,\#} \wedge x_{1,2,\sqcup} \wedge \cdots \wedge x_{1,2p(n)+2,\sqcup} \wedge x_{1,2p(n)+3,\#}$$

A Cook-Levin tétel bizonyítása

– φ_{move} akkor és csak akkor legyen igaz, ha minden ablak legális, azaz δ szerinti átmenetet ír le:

$$\varphi_{\text{move}} := \bigwedge_{\substack{1 \leq i \leq p(n) \\ 2 \leq j \leq 2p(n)+2}} \psi_{i,j},$$

ahol $\psi_{i,j} \sim \bigvee_{\substack{(b_1,\ldots,b_6) \\ \text{legális ablak}}} x_{i,j-1,b_1} \wedge x_{i,j,b_2} \wedge x_{i,j+1,b_3} \wedge$
$x_{i+1,j-1,b_4} \wedge x_{i+1,j,b_5} \wedge x_{i+1,j+1,b_6}$

b_1	b_2	b_3
b_4	b_5	b_6

De: $\psi_{i,j}$ sajnos nem KNF alakú!!! Ezért e helyett:

$$\psi_{i,j} := \bigwedge_{\substack{(b_1,\ldots,b_6) \\ \text{illegális ablak}}} \big(\neg x_{i,j-1,b_1} \vee \neg x_{i,j,b_2} \vee \neg x_{i,j+1,b_3} \vee \neg x_{i+1,j-1,b_4} \vee \neg x_{i+1,j,b_5} \vee \neg x_{i+1,j+1,b_6}\big)$$

A Cook-Levin tétel bizonyítása

– végezetül: φ_{accept} akkor és csak akkor legyen igaz, ha az utolsó sorban van q_i:

$$\varphi_{\text{accept}} = \bigvee_{j=2}^{2p(n)+2} x_{p(n)+1,j,q_i}$$

.

• $w \in L \Leftrightarrow$ az M NTG-nek van w-t elfogadó számítása$\Leftrightarrow$ T kitölthető úgy, hogy φ_w igaz $\Leftrightarrow$ φ_w kielégíthető $\Leftrightarrow \langle \varphi_w \rangle \in$ SAT,
• hány literált tartalmaz a φ_w formula? Legyen $k = |\Delta|$.
φ_0 : $(p(n)+1)(2p(n)+3)(k + k(k-1)) = O(p^2(n))$,
φ_{start} : $2p(n)+3 = O(p(n))$,
φ_{move} : $\leq p(n)(2p(n)+1)k^6 \cdot 6 = O(p^2(n))$,
φ_{accept} : $2p(n)+1 = O(p(n))$,
azaz φ_w $O(p^2(n))$ méretű, így polinom időben megkonstruálható
• tehát $w \mapsto \langle \varphi_w \rangle$ pol. idejű visszavezetés, így $L \leq_p$ SAT.
• Ez tetszőleges $L \in$ NP nyelvre elmondható. Így SAT NP-nehéz. Mivel NP-beli, ezért NP-teljes is.

Polinom idejű visszavezetés tranzitivitása

Állítás: $L_1 \leq_p L_2,\ L_2 \leq_p L_3 \Rightarrow L_1 \leq_p L_3$.

Bizonyítás:

Tartozzon az első visszavezetéshez egy f szófüggvény és legyen M_1 egy $p_1(n)$ idejű TG ami ezt kiszámítja. A másodikhoz tartozzon egy g függvény, melyet egy M_2 TG kiszámít $p_2(n)$ időben ($p_1(n)$ és $p_2(n)$ polinomok).

$w \in L_1 \Leftrightarrow f(w) \in L_2 \Leftrightarrow g(f(w)) \in L_3$, tehát $g \circ f$ visszavezetés.

$|f(w)| \leq n + p_1(n)$, ha $|w| = n$, ugyanis M_1 legfeljebb $p_1(n)$ darab lépést lesz, lépésenként $\leq$ 1-gyel nőhet a hossz.

Így $M_2 \circ M_1$ legfeljebb $h(n) := p_2(n + p_1(n))$ időben kiszámítja az $L_1 \leq L_3$-t bizonyító $g \circ f$-et.

Mivel $h(n)$ polinom, ezért $L_1 \leq_p L_3$.

További NP-teljes problémák

Az alábbi tétel alapján további nyelvek NP-teljességének bizonyítására nyílik lehetőség.

Tétel

Ha L NP-teljes, $L \leq_p L'$ és $L' \in$ NP, akkor L' NP-teljes.

Bizonyítás:

Legyen $L'' \in$ NP tetszőleges. Mivel L NP-teljes, ezért $L'' \leq_p L$. Mivel a feltételek szerint $L \leq_p L'$, ezért a polinom idejű visszavezetések tranzitivitása miatt L' NP-nehéz. Ebből és a 3. feltételből kövezkezik az állítás.

kSAT

Tehát a polinom idejű visszavezetés fogalmának segítségével további NP-beli nyelvek NP-teljessége bizonyítható. Erre nézzünk példákat.

KNF: konjuktív normálformájú nulladrendű formula

Volt: SAT=$\{\langle\varphi\rangle \mid \varphi$ kielégíthető KNF$\}$ NP-teljes.

Definíció

k**KNF**-nek nevezünk egy olyan KNF-t, ahol minden klóz pontosan k darab páronként különböző alapú literál diszjunkciója.

Példák 4KNF:

$(\neg x_1 \vee x_3 \vee x_5 \vee \neg x_6) \wedge (\neg x_1 \vee \neg x_3 \vee x_4 \vee \neg x_6) \wedge (x_1 \vee x_2 \vee \neg x_4 \vee \neg x_6)$.

2KNF: $(\neg x_1 \vee x_3) \wedge (\neg x_1 \vee \neg x_3) \wedge (x_1 \vee x_2) \wedge (\neg x_2 \vee x_3)$.

Definíció:

kSAT=$\{\langle\varphi\rangle \mid \varphi$ kielégíthető kKNF$\}$

3SAT NP-teljessége

Tétel

3SAT NP-teljes.

Bizonyítás:

- 3SAT NP-beli. Lásd az érvelést SAT-nál.
- SAT $\leq_p$ 3SAT
  Kell $f : \varphi \mapsto \varphi'$, φ KNF, φ' 3KNF, φ' kielégíthető $\Leftrightarrow \varphi$ kielégíthető, f polinom időben kiszámolható.

$\varphi \mapsto \varphi'$:

ℓ	$\ell \vee x \vee y,\ \ell \vee x \vee \neg y,\ \ell \vee \neg x \vee y,\ \ell \vee \neg x \vee \neg y$
$\ell_1 \vee \ell_2$	$\ell_1 \vee \ell_2 \vee x,\ \ \ell_1 \vee \ell_2 \vee \neg x$
$\ell_1 \vee \ell_2 \vee \ell_3$	$\ell_1 \vee \ell_2 \vee \ell_3$
$\ell_1 \vee \ell_2 \vee \ell_3 \vee \ell_4$	$\ell_1 \vee \ell_2 \vee x,\ \ \neg x \vee \ell_3 \vee \ell_4$
$\ell_1 \vee \cdots \vee \ell_n\ (n \geq 5)$	$\ell_1 \vee \ell_2 \vee x_1, \neg x_1 \vee \ell_3 \vee x_2, \ldots, \neg x_{n-3} \vee \ell_{n-1} \vee \ell_n$

$x, y, x_1, \ldots, x_{n-3}$ új ítéletváltozók.

Minden tagra elvégezzük a fenti helyettesítést. φ' ezek konjunkciója.

3SAT NP-teljessége

ℓ	$\ell \vee x \vee y,\ \ell \vee x \vee \neg y,\ \ell \vee \neg x \vee y,\ \ell \vee \neg x \vee \neg y$
$\ell_1 \vee \ell_2$	$\ell_1 \vee \ell_2 \vee x,\ \ \ell_1 \vee \ell_2 \vee \neg x$
$\ell_1 \vee \ell_2 \vee \ell_3$	$\ell_1 \vee \ell_2 \vee \ell_3$
$\ell_1 \vee \ell_2 \vee \ell_3 \vee \ell_4$	$\ell_1 \vee \ell_2 \vee x,\ \ \neg x \vee \ell_3 \vee \ell_4$
$\ell_1 \vee \cdots \vee \ell_n\ (n \geq 5)$	$\ell_1 \vee \ell_2 \vee x_1, \neg x_1 \vee \ell_3 \vee x_2, \ldots, \neg x_{n-3} \vee \ell_{n-1} \vee \ell_n$

Belátjuk, hogy ha egy I interpretáció kielégíti φ-t, akkor az új változók megfelelő kiértékelésével megadható egy I' φ'-t kielégítő interpretáció.

És fordítva, ha adott egy I' φ'-t kielégítő interpretáció, akkor ennek a régi változókra való I megszorítása kielégíti φ-t.

Az állításokat tagonként gondoljuk meg. Tekintsük φ egy n literálból álló tagját.

$n = 3$: nincs bizonyítani való

$n = 2$: $(\Rightarrow)$: ha legalább az egyik literál igaz, nyilván mindkét jobboldali tag igaz $(\Leftarrow)$: x és $\neg x$ közül az egyik hamis, így ha mindkét jobboldali tag igaz, akkor ℓ_1 vagy ℓ_2 igaz.

3SAT NP-teljessége

ℓ	$\ell \vee x \vee y,\ \ell \vee x \vee \neg y,\ \ell \vee \neg x \vee y,\ \ell \vee \neg x \vee \neg y$
$\ell_1 \vee \ell_2$	$\ell_1 \vee \ell_2 \vee x,\ \ \ell_1 \vee \ell_2 \vee \neg x$
$\ell_1 \vee \ell_2 \vee \ell_3$	$\ell_1 \vee \ell_2 \vee \ell_3$
$\ell_1 \vee \ell_2 \vee \ell_3 \vee \ell_4$	$\ell_1 \vee \ell_2 \vee x,\ \ \neg x \vee \ell_3 \vee \ell_4$
$\ell_1 \vee \cdots \vee \ell_n\ (n \geq 5)$	$\ell_1 \vee \ell_2 \vee x_1, \neg x_1 \vee \ell_3 \vee x_2, \ldots, \neg x_{n-3} \vee \ell_{n-1} \vee \ell_n$

$n=1$: ($\Rightarrow$): ha ℓ igaz, nyilván minden jobboldali tag igaz ($\Leftarrow$): "$\ell \vee$" nélkül nem lehet mindegyik egyszerre igaz. Így ha minden jobboldali tag igaz, akkor ℓ igaz.

$n=4$: ($\Rightarrow$): ha a 4 közül valamelyik literál igaz, akkor igaz az egyik jobboldali tag. x igazságértékét válasszuk úgy, hogy a másik tag is igaz legyen. ($\Leftarrow$): x és $\neg x$ közül az egyik hamis, így ha mindkét jobboldali tag igaz, akkor $\ell_1, \ell_2, \ell_3, \ell_4$ közül legalább egy igaz.

$n \geq 5$: ($\Rightarrow$): Tegyük fel, hogy ℓ_i igaz. Ekkor legyen $x_1, \ldots, x_{i-2}$ igaz $x_{i-1}, \ldots, x_{n-3}$ hamis. Átgondolható, hogy minden tagban lesz igaz literál.

3SAT NP-teljessége

ℓ	$\ell \vee x \vee y,\ \ell \vee x \vee \neg y,\ \ell \vee \neg x \vee y,\ \ell \vee \neg x \vee \neg y$
$\ell_1 \vee \ell_2$	$\ell_1 \vee \ell_2 \vee x,\ \ \ell_1 \vee \ell_2 \vee \neg x$
$\ell_1 \vee \ell_2 \vee \ell_3$	$\ell_1 \vee \ell_2 \vee \ell_3$
$\ell_1 \vee \ell_2 \vee \ell_3 \vee \ell_4$	$\ell_1 \vee \ell_2 \vee x,\ \ \neg x \vee \ell_3 \vee \ell_4$
$\ell_1 \vee \cdots \vee \ell_n\ (n \geq 5)$	$\ell_1 \vee \ell_2 \vee x_1, \neg x_1 \vee \ell_3 \vee x_2, \ldots, \neg x_{n-3} \vee \ell_{n-1} \vee \ell_n$

$n \geq 5$: ($\Leftarrow$): Tegyük fel, hogy jobboldalon minden tag igaz és indirekt tegyük fel, hogy $\ell_1, \ldots, \ell_n$ hamis. Ekkor az új tagokon balról jobbra végighaladva sorra kapjuk, hogy $x_1, \ldots x_{n-3}$ igaz kell legyen, de ekkor az uolsó tag mégiscsak hamis, ellentmondás.

Tehát φ kielégíthető $\Leftrightarrow$ φ' kielégíthető. φ' φ-ből polinom időben elkészíthető és mérete az eredeti méret polinomja, tehát SAT$\leq_p$ 3SAT.

2SAT P-beli

Tétel

2SAT $\in$ P.

Bizonyítás Legyen φ egy $x_1, \ldots, x_n$ változókat tartalmazó 2KNF formula m klózzal.

Konstruálunk egy G_φ $2n$ csúcsú irányított gráfot. G_φ csúcsai legyenek a $2n$ literál és minden $\ell_i \vee \ell_j$ klóz esetén adjuk hozzá a $(\neg \ell_i, \ell_j)$ és a $(\neg \ell_j, \ell_i)$ irányított éleket a gráf élhalmazához. Ezt az motiválja, hogy $\ell_i \vee \ell_j \sim_0 \neg \ell_i \to \ell_j \sim_0 \neg \ell_j \to \ell_i$.

Be fogjuk látni a következő állítást:

Állítás: φ akkor és csak akkor kielégíthető, ha G_φ egyetlen erősen összefüggő komponense se tartalmaz komplemens literálpárt.

(Emlékeztető: egy irányított gráf erősen összefüggő, ha bármely két csúcsa között van mindkét irányban irányított út. Minden irányított gráf csúcshalmaza erősen összefüggő komponensekre particionálható.)

2SAT P-beli

Az állításból következik a tétel, hiszen ismeretes (lásd pl. Algoritmusok és Adatszerkezetek II.), hogy egy $G = (V, E)$ gráf erősen összefüggő komponensei $O(|V| + |E|)$ időben meghatározhatóak, és most $|V| = 2n, |E| = 2m$, azaz az algoritmus $\max\{n, m\}$-ben polinomiális.

Az állítás bizonyítása: Vegyük észre, hogy ha egy I interpretáció kielégíti φ-t, akkor ha egy literál igaz I-ben, akkor minden belőle kiinduló él végpontja is igaz. Így az erősen összefüggő komponensek literáljainak ugyanaz az igazságértéke.

Ebből azonnal következik az állítás egyik iránya, hiszen ha G_φ valamelyik erősen összefüggő komponense tartalmaz komplemens literálpárt, akkor ezen literálpárnak ugyanaz lenne az igazságértéke, ami lehetetlen. Így φ kielégíthetetlen.

2SAT P-beli

Az állítás másik irányához meg kell adnunk egy φ-t kielégítő I interpretációt ha G_φ erősen összefüggő komponensei nem tartalmaznak komplemens literálpárt.

Legyen x_i tetszőleges ítéletváltozó. A feltétel szerint vagy x_i-ből $\neg x_i$-be vagy $\neg x_i$-ből x_i-be nincs irányított út. Ha egyik sincs, akkor adjuk hozzá G_φ-hez az $e = (x_i, \neg x_i)$ élt.

Ettől nem sérül a feltétel, hiszen ha ezzel valamely j-re x_j és $\neg x_j$ egy komponensbe kerülne, akkor ide kerülne az e él is és így x_i és $\neg x_i$ is. Azonban ez nem lehet, hiszen nincs $\neg x_i$-ből x_i-be út.

Ezt addig folytatjuk, amíg nem lesz G_φ-ben minden komplemens literálpár között pontosan az egyik irányba út. Minden i-re

$$I(x_i) := \begin{cases} i, & \text{ha } G_\varphi\text{-ben van } \neg x_i\text{-ből } x_i\text{-be irányított út} \\ h & \text{ha } G_\varphi\text{-ben van } x_i\text{-ből } \neg x_i\text{-be irányított út} \end{cases}$$

Így minden hamis literálból van a komplemens párjába irányított út.

2SAT P-beli

Ez az I interpretáció minden klózt igazra értékel.

Ugyanis indirekt tegyük fel, hogy φ-nek az $\ell_i \vee \ell_j$ klóza I-ben hamis. Ekkor ℓ_i és ℓ_j is hamis. Tehát az I definíciója utáni észrevétel miatt

(1) van irányított út ℓ_i-ből $\neg\ell_i$-be és ℓ_j-ből $\neg\ell_j$-be.

Másrészt G_φ definíciója miatt

(2) $(\neg\ell_i, \ell_j)$ és $(\neg\ell_j, \ell_i)$ éle G_φ-nek.

(1)-ből és (2)-ből következik, hogy ℓ_i és $\neg\ell_i$ G_φ-nek ugyanabban az erősen összefüggő komponensében van, ami feltételünk szerint nem lehet.

Ezzel az állítás és így a tétel bizonyítását is befejeztük.

HORNSAT P-beli

Definíció

Horn formula: olyan KNF, amelynek minden tagja legfeljebb egy pozitív (azaz negálatlan) literált tartalmaz.

Példa: $(\neg x_1 \vee x_3) \wedge (\neg x_1 \vee \neg x_3 \vee x_4 \vee \neg x_6) \wedge (\neg x_2 \vee \neg x_4 \vee \neg x_6)$

$\mathrm{HORNSAT} = \{\langle\varphi\rangle \mid \varphi$ kielégíthető Horn formula$\}$

Tétel

$\mathrm{HORNSAT} \in \mathrm{P}$.

Nem bizonyítjuk.